needs Ch #1, 2, 3, 4, & 5

OPNAV INSTRUCTION 5510.1B

DEPARTMENT OF THE NAVY

SECURITY MANUAL FOR CLASSIFIED INFORMATION

NAVY DEPARTMENT
CHIEF OF NAVAL OPERATIONS
OFFICE OF NAVAL INTELLIGENCE

OPNAV INSTRUCTION 5510.1B

DEPARTMENT OF THE NAVY

SECURITY MANUAL FOR CLASSIFIED INFORMATION

NAVY DEPARTMENT
CHIEF OF NAVAL OPERATIONS
OFFICE OF NAVAL INTELLIGENCE

I

DEPARTMENT OF THE NAVY
Office of the Chief of Naval Operations
Washington 25, D. C.

OPNAV 5510.1B
Op-921B
Ser 550P92

10 MAR 1958

OPNAV INSTRUCTION 5510.1B

From: Chief of Naval Operations
To: All Ships and Stations

Subj: Department of the Navy Security Manual for Classified Information

1. Purpose. The purpose of this Instruction is to provide all Naval activities and personnel with detailed regulations and guidance for classifying, marking and handling classified information and for access thereto and disclosure thereof.

2. Cancellation. OPNAV INSTRUCTION 5510.1A (U.S. Navy Security Manual for Classified Matter) is hereby cancelled and superseded.

3. Scope. This Instruction serves as the basic U. S. Navy security directive relating to the safeguarding of classified information. Its provisions apply to all military and civilian personnel and to all activities of the Naval Establishment.

4. Procurement. Navy and Marine Corps activities may procure additional copies of this Instruction by submitting a "Requisition and Invoice/Shipping Document" (DD Form 1149) to the nearest Forms and Publications Supply Distribution Point.

H. D. Felt

H. D. FELT
VICE CHIEF OF NAVAL OPERATIONS

Approved: 12 MAR 1958

W. B. Franke

Under Secretary of the Navy

TABLE OF CONTENTS

	Page
Chapter 1 — Introduction	1-1
Chapter 2 — Definitions	2-1
Chapter 3 — Classification Categories	3-1
Chapter 4 — Classification, Preparation and Marking:	
Section 1 — Basic Instructions	4-1
Section 2 — Change in Classification	4-5
Section 3 — Preparation and Marking	4-6
Chapter 5 — Control Officers:	
Section 1 — Classified Material Control Officers	5-1
Section 2 — Top Secret Control Officers	5-1
Chapter 6 — Custody:	
Section 1 — Stowage	6-1
Section 2 — Accounting	6-7
Section 3 — Custodial Precautions	6-8
Section 4 — Disposition of Classified Material	6-10
Section 5 — Destruction of Classified Material	6-10
Chapter 7 — Transmission:	
Section 1 — Methods of Transmission	7-1
Section 2 — Transmission by Courier	7-5
Section 3 — Preparation of Material for Transmission	7-6
Chapter 8 — Security Violations and Compromises	8-1
Chapter 9 — Control of Dissemination:	
Section 1 — General	9-1
Section 2 — Oral Discussion and Personal Censorship	9-3
Section 3 — Disclosure Through Judicial Proceedings	9-5
Section 4 — Disclosure to Foreign Governments	9-7
Section 5 — Disclosure Outside the Executive Branch	9-8
Section 6 — Disclosure Through Conferences and Symposia	9-9
Chapter 10 — Disclosure Through Public Relations	10-1
Chapter 11 — Control of Photography	11-1
Chapter 12 — Reproduction of Classified Information	12-1
Chapter 13 — Communication Security	13-1
Chapter 14 — Visitor Control:	
Section 1 — General	14-1
Section 2 — Unclassified Visits	14-2
Section 3 — Classified Visits	14-5
Chapter 15 — Personnel Security Investigations and Clearances for Access to Classified Information:	
Section 1 — Personnel Security Investigations	15-1
Section 2 — Personnel Security Clearances	15-3
Appendix A — Procurement of Forms	A-1
Appendix B — Atomic Energy Act of 1954	B-1
Appendix C — Executive Order 10450	C-1
Appendix D — Espionage and Censorship	D-1
Appendix E — Executive Order 10104	E-1
Appendix F — Cryptographic Systems	F-1
Appendix G — Employment Suspension	G-1
Appendix H — Internal Security Act of 1950	H-1
Appendix I — Protective Alarm Systems	I-1
Appendix J — Security Areas	J-1
Index	INDEX-1

LIST OF EFFECTIVE PAGES

Subject Matter	*Effective Pages*	*Page Numbers*
Title Page	Original	I (reverse blank)
Letter of Promulgation	Original	III (reverse blank)
Table of Contents	Original	V (reverse blank)
List of Effective Pages	Original	VII (reverse blank)
Record of Corrections	Original	IX (reverse blank)
Chapter 1	Original	1–1, 1–2
Chapter 2	Original	2–1 — 2–4
Chapter 3	Original	3–1 — 3–4
Chapter 4	Original	4–1 — 4–10
Chapter 5	Original	5–1, 5–2
Chapter 6	Original	6–1 — 6–12
Chapter 7	Original	7–1 — 7–7 (reverse blank)
Chapter 8	Original	8–1, 8–2
Chapter 9	Original	9–1 — 9–10
Chapter 10	Original	10–1, 10–2
Chapter 11	Original	11–1, 11–2
Chapter 12	Original	12–1 (reverse blank)
Chapter 13	Original	13–1, 13–2
Chapter 14	Original	14–1 — 14–8
Chapter 15	Original	15–1 — 15–12
Appendix A	Original	A–1 (reverse blank)
Appendix B	Original	B–1 — B–5 (reverse blank)
Appendix C	Original	C–1 — C–6
Appendix D	Original	D–1 — D–3 (reverse blank)
Appendix E	Original	E–1, E–2
Appendix F	Original	F–1 (reverse blank)
Appendix G	Original	G–1, G–2
Appendix H	Original	H–1, H–2
Appendix I	Original	I–1 — I–3 (reverse blank)
Appendix J	Original	J–1, J–2
Index	Original	Index–1 — Index–22

RECORD OF CORRECTIONS

Identification of correction or change	Date entered	By whom entered (signature; rank or rate; name of command)
[redacted]		

Chapter 1
INTRODUCTION

0101. RESPONSIBILITY

1. The Chief of Naval Operations is responsible to the Secretary of the Navy for all policies relating to the maintenance of the security of all classified information within the Naval Establishment. Owing to the close relationship of counterintelligence and the preservation of security, the Director of Naval Intelligence has been designated as the officer primarily responsible to the Chief of Naval Operations for the protection of classified information. Therefore, the Office of Naval Intelligence formulates and promulgates Navy policies which relate to the security of all classified information.
2. Commanding officers are directly responsible for safeguarding all classified information within their commands and are responsible for instructing their personnel in security practices and procedures.

0102. OBJECTIVE

1. The objective of the orders and instructions which appear herein is to establish a coordinated policy for the maintenance of the security of all information classified in the interests of national defense.
2. Information which requires administrative protection for reasons other than in the interests of national defense is not classified information as defined in this Instruction and the protective measures established herein do not apply. Originators of such information are responsible for insuring its identification and protection in accordance with existing regulations. Under no circumstances shall the designation Top Secret, Secret, or Confidential (including Confidential-Modified Handling Authorized) be assigned to such information.

0103. APPLICATION

The security of the United States in general, and of naval operations in particular, depends in part upon the success attained in the safeguarding of classified information. It is of paramount importance that all who engage in administering security preserve a balanced and commonsense outlook toward the subject. The ideal to be sought is the indoctrination of all personnel to the point that they automatically exercise proper discretion in the discharge of their duties and do not think of security of information as something separate and apart from other things. In this way, security of classified information becomes a natural element of every task and not an additionally imposed burden. The attainment of the desired objective requires sound direction from above and full alertness and cooperativeness on the part of all subordinates.

0104. BASIS

U. S. Navy Regulations and General Orders, Executive Orders, public laws, and other legally established directives form the basis for this publication.

0105. LIMITATIONS OF SECURITY

Security is a means — not an end. Rules which govern security of classified information are comparable to gunnery safety orders. They do not guarantee protection, and they do not attempt to meet every conceivable situation. The law of diminishing returns limits the control measures that can be employed profitably, but it is possible to obtain a satisfactory degree of security with a minimum of sacrifice in operating efficiency.

0106. SECURITY PRINCIPLE

The Department of Defense is employing a security formula which is simple in principle. It is based on the premise of circulation control; i.e., the control of the dissemination of classified information. Therefore, knowledge or possession of

classified defense information shall be permitted only to persons whose official duties require such access in the interest of promoting national defense and only if they have been determined to be trustworthy.

0107. GENERAL INTERPRETATION

In the interpretation of the provisions of this publication, each command and individual shall be guided by the basic principle of security. The regulations contained herein are not intended to restrict the mature judgment of individuals in the proper application of initiative. It is directed that commands issue additional security instructions as necessary to meet local situations.

0108. FORMS

Except where specifically indicated, forms required by this Manual may be obtained by forwarding DD Form 1149 (Requisition and Invoice/Shipping Documents) direct to appropriate forms and publications supply points. (Refer to Appendix A).

Chapter 2
DEFINITIONS

0201. ACCESS

"Access" is the ability and opportunity to obtain knowledge or possession of classified information. An individual does not have access to classified information merely by being in a place where such information is kept, provided the security measures which are in effect prevent him from gaining knowledge or possession of such classified information.

0202. BOUND DOCUMENTS

"Bound Documents" are books or pamphlets, the pages of which are permanently and securely fastened together in such a manner that one or more pages cannot be extracted from the bound copy without defacement or alteration of the book.

0203. CATEGORIES OF CLASSIFIED INFORMATION

There are three categories of classified information which, in descending order of importance, shall carry one of the following designations: "Top Secret," "Secret," or "Confidential" (including Confidential-Modified Handling Authorized).

0204. CLASSIFICATION GUIDE

An instruction indicating the classification that may be assigned to subjects within a specific area of defense activity.

0205. CLASSIFIED INFORMATION

"Classified information" is official information which requires protection in the interests of National defense and which is classified for such purpose by responsible classifying authority.

0206. CLASSIFIED MATERIAL

"Classified material" is any matter, document, product, or substance on or in which classified information is recorded or embodied.

0207. CLASSIFIED MATTER

Refer to article 0206. (The terms "classified information", "classified material" and "classified matter" are sometimes used as synonyms in other regulatory publications. The instant differentiation between "classified information" (article 0205) and "classified material" or "classified matter" (articles 0206–0207) is not intended to interfere with that broader meaning wherever employed.)

0208. CLASSIFY

To "classify" is the procedure whereby (1) a decision is made to place information within a classification category after it is first determined that the information requires protection in the interests of national defense, (2) the classified information is marked accordingly, and (3) interested commands are notified as to the assigned classification.

0209. CLEARANCE

A "clearance" is an administrative determination by competent authority that an individual is eligible, from a security standpoint, for access to classified information of a specified category.

0210. COMMUNICATION SECURITY

"Communication security" is protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from communications.

0211. COMPARTMENTALIZATION (CIRCULATION CONTROL)

The rules and regulations established by competent authority to insure that access to classified information will be granted only to trustworthy persons who require such information in performance of

their official duties and classified information is restricted to specific physical confines when feasible.

0212. COMPETENT AUTHORITY—COMMANDING OFFICER

For the purposes of this Instruction, the terms "competent authority" and "commanding officer" are synonymous. These terms are intended to include "commander", "officer-in-charge", "naval representative", "director", "inspector", and any other title assigned to an individual, military or civilian, who, through command status position, or administrative jurisdiction, is qualified to assume responsibility and to render a decision with regard to a specific question under consideration.

0213. COMPROMISE

A "compromise" is a loss of security which results from an unauthorized person obtaining knowledge of classified information. As used in this Instruction, the term "unauthorized person" means any person not authorized to have access to classified information.

0214. CONFIDENTIAL (CONFIDENTIAL-MODIFIED HANDLING AUTHORIZED)

Refer to article 0304.

0215. COUNTERINTELLIGENCE

"Counterintelligence" is that phase of intelligence covering all activity devoted to destroying the effectiveness of inimical foreign intelligence activities and to the protection of information against espionage, personnel against subversion, and installations or material against sabotage.

0216. DECLASSIFY

To "declassify" is to remove the classification from classified information. Notification to holders of the information is a part of this process.

J217. DISCLOSURE

"Disclosure," as it relates to classified information, is an officially authorized release or dissemination by competent authority whereby the information is furnished to a specific individual, group, or activity.

0218. DOCUMENT

The term "document" means any recorded information, regardless of its physical form or characteristics, and includes but is not limited to the following:

1. Written material, whether handwritten, printed or typed.
2. All painted, drawn or engraved material.
3. All sound or voice recordings.
4. All printed photographs and exposed or printed film, still or motion pictures.
5. All reproductions of the foregoing by whatever process reproduced.

0219. DOWNGRADING

"Downgrading" is the act of lowering the classification assigned to information while retaining it within a category of classified information. Notification to holders of the information is a part of the process.

0220. FOR OFFICIAL USE ONLY

The term "For Official Use Only" is assigned to official information which requires protection in accordance with statutory requirements or in the public interest, but which is not within the purview of the rules for safeguarding information in the interests of national defense. Such information is *not* within the purview of this Instruction; its description, use and limitations are set forth in SECNAV Instruction 5570.2A.

0221. FOREIGN NATIONAL

The term "foreign national" includes any person not a U. S. citizen or U. S. national. American citizens representing foreign governments, foreign private interests, or other foreign nationals are considered to be foreign nationals for purposes of this Instruction.

0222. FORMERLY RESTRICTED DATA

Refer to article 0305.2.

0223. HANDLING

The term "handling" includes the preparation, processing, transmission, and custody of classified information.

0224. IMMIGRANT ALIEN

An "immigrant alien" is any person who has been lawfully admitted into the United States for permanent residence under an immigration visa. (See Article 1507 for investigative requirements for clearances for "immigrant aliens" within the Naval Establishment.)

0225. INFORMATION

"Information" is knowledge which can be communicated by any means.

0226. INTERNATIONAL DOCUMENTS

Classified material marked by such terms as "COSMIC", "NATO", "SEATO", and "BAGHDAD PACT" is handled in accordance with separate instructions established by the particular organization. Opnav Instruction 05510.46 sets forth the handling requirements for COSMIC and NATO classified information; OPNAV Instruction 05510.53 provides similar guidance for SEATO classified information and 05510.54 for BAGHDAD PACT classified information.

0227. LONG TITLE

"Long title" is a descriptive word or phrase, consisting of a name or of several words, assigned by the preparing agency to identify the subject matter of a document on the type of device.

0228. MARKING

"Marking" is the physical act of indicating on classified material the assigned classification, changes in classification, and any special limitations on the use thereof.

0229. MUNITIONS OF WAR

The term "munitions of war" includes any and all items required for war, inclusive of food as well as all other supplies and equipment, but exclusive of manpower.

0230. NEED TO KNOW

"Need to know" is the term given to the requirement that the dissemination of classified information be limited strictly to those persons whose official military or other governmental duties require knowledge or possession thereof. Responsibility for determining whether a person's duties require that he possess or have access to classified information and whether he is authorized to receive it rests upon each individual who has possession, knowledge, or command control of the information involved and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a command, a defense contractor, another Federal agency, or a foreign government. A "need to know" is recognized as established when (1) the disclosure is necessary in the interests of national defense; (2) there clearly appears from the position, status, duties, and responsibilities of the applicant a legitimate requirement that he must have access to the classified information in order to carry out his assigned duties and responsibilities; (3) there is no other equal or ready source of the same classified information available to him; and (4) the applicant is or can be appropriately cleared for accesss to the degree of classified information involved and is capable both physically and mentally of providing the degree of protection which that information requires.

0231. ORIGINAL CLASSIFICATION AUTHORITY

"Original classification authority" is that authority required to classify independently any type of material; this contrasts with derivative classification authority, which is the authority to classify material created as a result of, in connection with, or in response to other material dealing with the same subject which already bears a classification.

0232. ORIGINATOR

The "originator" is the command by whose authority an item of information is created and disseminated.

0233. PERSONNEL SECURITY CLEARANCE

A "personnel security clearance" is an administrative determination that an individual is eligible, from a security standpoint, for access to classified information of the same or lower category as the clearance being granted.

0234. RECLASSIFYING OR REGRADING

"Reclassifying" or "regrading" is the act of changing the classification assigned to information. Notification to holders of the information is a part of the process.

0235. RESTRICTED DATA

Refer to article 0305.

0236. SECRET

Refer to article 0303.

0237. SECURITY

"Security" is a protected condition of classified information which prevents unauthorized persons from obtaining information of direct or indirect military value. This condition results from the establishment and maintenance of protective measures which insure a state of inviolability from hostile acts or influences.

0238. SHORT TITLE

A "short title" is a brief, identifying combination of words, letters, or numbers applied to specific items of classified material.

0239. SPONSORSHIP

"Sponsorship" (or other forms of the word) is used herein to indicate that a command or activity officially accepts responsibility, securitywise, for an individual, a group, conference, etc. Usually a "sponsored" individual is a member of the "sponsoring command" (i.e., all members of a command visiting anywhere officially are prima facie sponsored by their own command), but this is not necessarily the case. "Sponsored" individuals, groups, etc. may include members of the Naval Establishment, other military departments and other branches of the Government; contractors and their employees; other American citizens; and foreign nationals. Sponsorship should not lightly be undertaken.

0240. STOWAGE

"Stowage" refers to the manner in which classified material is protected by physical and/or mechanical means.

0241. TECHNICAL INFORMATION

"Technical information" includes data concerning munitions and equipment, engineering performance, instructions on maintenance and operation, and any descriptive matter or components thereof. The term also includes means of operation, manufacture, use, techniques, processes, and information pertaining to the various sciences which may be employed directly or indirectly in warfare. Data of a strategic or tactical nature are specifically excluded from the meaning of this term.

0242. TOP SECRET

Refer to article 0302.

0243. TRANSMISSION

"Transmission" (including transmit, transmitting, transmittal and other forms of the word) as used in this Instruction means movement involving the actual transfer of custody and responsibility for a document or other classified material from one command or section of a command to another command or other authorized addressee. It does not apply to personnel carrying classified material for their own legitimate use to be retained by them and returned to their own command files.

0244. UNBOUND DOCUMENTS

"Unbound documents" include letters, memoranda, reports, telegrams, and other similar documents the pages of which are not permanently and securely fastened together.

0245. UPGRADING

"Upgrading" is the act of assigning a higher classification to information than that previously assigned. Notification to holders of the information is a part of this process.

Chapter 3
CLASSIFICATION CATEGORIES

0301. GENERAL

1. Official information which requires protection in the interests of national defense shall be limited to three categories of classification which, in descending order of importance, shall carry one of the following designations: Top Secret, Secret, or Confidential (including Confidential-Modified Handling Authorized). No other designation shall be used to classify defense information, as requiring protection in the interests of national defense, except as expressly provided by statute. Official information not affecting the national defense, which pursuant to statutory or constitutional authority may be deemed to require protection in the public interest for other reasons, shall be handled in accordance with SECNAV Instruction 5570.2A.

2. Nothing in this Instruction shall be deemed to authorize the withholding of information, otherwise releasable, because its release might tend to reveal administrative error or inefficiency, or might be embarrassing.

0302. DEFINITION OF TOP SECRET

The use of the classification Top Secret shall be limited to defense information or material which requires the highest degree of protection. The Top Secret classification shall be applied only to that information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation, such as:

1. Leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its Allies, a war.

2. The compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.

3. Examples of the type of material described in subparagraphs 1 and 2 above might include the following:

a. A strategic plan documenting the overall conduct of a war.

b. War planning documents which contain worldwide:

(1) Planning data and assumptions.

(2) Wartime planning factors for the use of nuclear weapons.

(3) Intelligence estimates of enemy capabilities.

(4) Force composition and deployment, and

(5) Real estate requirements and utilization by geographical area which are time phased for a period of months.

c. An operations plan either for a single operation or a series of connected operations containing any of the factors in subparagraph *b* above and with sortie rates or target data.

d. A document containing any of the considerations in subparagraph *b* above directly related to a Top Secret war planning document, the unauthorized disclosure of which standing alone could result in actual compromise of a particular Top Secret plan. (This does not necessarily include proposed budgets, current peacetime deployment of units or munitions, or peacetime manpower and organization programs for future years. Normally such information is too general in nature to reveal Top Secret plans.)

e. Intelligence documents that contain completed intelligence of such scope that it reveals a major intelligence production effort on the part of the United States and which would permit an evaluation by unauthorized recipients of the success attained by, or the capabilities by, or the capabilities of, the United States intelligence services. (Normally, a broad and complete intelligence annex or a summary of

similar importance. Not a report or a digest of reported items of information, except as covered in subparagraph *f* below.)

f. A plan or policy for conducting intelligence or other special operations and information revealing a particular intelligence operation or other special operation, provided that the compromise of such plan, policy, or particular operation could result in exceptionally grave damage to the Nation — not just to individuals or groups of individuals. Intelligence operations may include certain specifically designated and controlled collection projects.

g. Critical information concerning radically new and extremely important equipment (munitions of war), such as nuclear weapons, atomic weapons stockpile data, and any other munitions of comparable importance the scientific or technological development aspects of which are vital to the national defense. (OPNAV INSTRUCTION 005510.2B (and subsequent revisions), AEC-DOD Classification Guide, applies to Restricted Data, and also indicates the proper defense classification for the same information.)

0303. DEFINITION OF SECRET

The use of the classification Secret shall be limited to defense information or material the unauthorized disclosure of which could result in serious damage to the Nation, such as:

1. Jeopardizing the international relations of the United States.
2. Endangering the effectiveness of a program or policy of vital importance to the national defense.
3. Compromising important military or defense plans, or scientific or technological developments important to national defense.
4. Revealing important intelligence operations.
5. Examples of the type of material described in subparagraphs 1 through 4 above might be the following:

a. A war plan or a complete plan for a future operation of war not included under Top Secret, and documents showing the disposition of our forces the unauthorized disclosure of which, standing alone, could result in actual compromise of such Secret plans.

b. Defense or other military plans not included under Top Secret or subparagraph *a*, above, including certain development and procurement plans and programs, but not necessarily including all emergency plans.

c. Specific information which, standing alone, reveals the military capabilities or state of preparedness of the Armed Forces, but not including information the unauthorized disclosure of which could result in compromise of a Top Secret plan.

d. Information that reveals the strength of our forces engaged in hostilities; quantities or nature of their equipment; or the identity or composition of units in an active theater of operations or other geographic area where our forces are engaged in hostilities, except that mailing addresses may include organization designations. (During periods of peace, information revealing the strength, identity, composition, or location of units normally does not require classification as Secret.)

e. Intelligence and other information, the value of which depends upon concealing the fact that the United States possesses it.

f. Particulars of scientific or research projects which incorporate new technological developments or techniques having direct military application of vital importance to the national defense.

g. Specific details or data relating to new material or important modifications of material which reveal significant military advances or new technological developments having direct military application of vital importance to the national defense.

h. Communications security devices and cryptographic material that reveals information of vital importance to the national defense.

i. Information of vital importance to the national defense concerning specific quantities of war reserves.

0304. DEFINITION OF CONFIDENTIAL (CONFIDENTIAL—MODIFIED HANDLING AUTHORIZED)

1. The use of the classification Confidential shall be limited to defense information or material the

unauthorized disclosure of which could be prejudicial to the defense interests of the Nation. Examples of the type of material described might include the following:

a. Operational and battle reports which contain information of value to the enemy.

b. Intelligence reports.

c. Military radio frequency and call sign allocations of special significance or those which are changed frequently for security reasons.

d. Devices and material relating to communications security.

e. Information which indicates strength of our ground, air and naval forces in United States and overseas areas, identity or composition of units, or quantity of specific items of equipment pertaining thereto. (During periods of peace, a defense classification is not necessarily required, unless such information reflects the overall strength figures or quantities of weapons whose characteristics are themselves classified, or additional factors necessitate security protection.)

f. Documents and manuals containing technical information used for training, maintenance and inspection of classified munitions of war.

g. Operational and tactical doctrine.

h. Research, development, production; and procurement of munitions of war.

i. Mobilization plans.

j. Personnel security investigations and other investigations which require protection against unauthorized disclosure.

k. Matters and documents of a personal and disciplinary nature, the disclosure of which could be prejudicial to discipline and morale of the Armed Forces.

l. Documents used in connection with procurement, selection and promotions of military personnel, the disclosure of which could violate the integrity of the competitive system.

NOTE: While in all of the above cases, the assignment of Confidential must be justified, particular care must be exercised with respect to paragraphs j, k and l above to make certain that such matters are assigned to the Confidential category only if in fact the unauthorized disclosure of such information could be prejudicial to the defense interests of the nation. If such information is not strictly defense information but nevertheless requires protection, it will be safeguarded by the application of the provisions of SECNAV INSTRUCTION 5570.2A and subsequent revisions.

2. Confidential defense information, as defined above, pertaining to combat or combat-related operations, actual or simulated, may be identified by the term "Confidential-Modified Handling Authorized". The lesser security safeguards for stowage and transmission prescribed in Articles 0602, 0702, and 0711 does not preclude a more secure means if desired. Except as specifically authorized in the above referenced articles, material designated "Confidential-Modified Handling Authorized" shall be subject to all the requirements in this Manual specified for "Confidential" defense information.

a. Combat or combat-related operations, actual or simulated, as used herein relate to military planning, operations, training, communications and the logistical support thereof.

b. Examples of such information might include the following:

(1) Training, Field and Technical Manuals and related material.

(2) Photographs, negatives, photostats, diagrams or material.

(3) Defense procurement plans, including procurement contracts and related matters.

(4) Communications material and messages.

(5) Certain documents regarding engineering plans and design details, computation, method of processing or assembling, which are essential to the functioning or use of an article of material.

(6) Military maps and aerial photography, and related material, which require wide dissemination for military purposes.

(7) Information received from foreign nations under existing international exchange of information agreements and policies, and classified "Restricted" by them.

0305. DEFINITION OF RESTRICTED DATA AND FORMERLY RESTRICTED DATA

1. The term "RESTRICTED DATA" as defined in the Atomic Energy Act of 1954 (42 USC 2011 et seq.; refer to Apendix B) means all data concerning (1) the design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RESTRICTED DATA category which the Atomic Energy Commission from time to time determines may be published without undue risk to the common defense and security.

2. The term "FORMERLY RESTRICTED DATA" applies to that classified defense information which (a) has been removed from the RESTRICTED DATA category under Section 142d, Atomic Energy Act of 1954 and (b) cannot be released to foreign nationals except under specific international agreements. Such information will be marked as follows:

FORMERLY RESTRICTED DATA

Handle as Restricted Data in Foreign Dissemination
Section 144b, Atomic Energy Act, 1954

(Note that such information *may* be releasable and should *not* be marked in the same manner as classified material not releasable to foreign nationals in accordance with article 0423.)

Chapter 4
CLASSIFICATION, PREPARATION AND MARKING
Section 1
BASIC INSTRUCTIONS

0401. AUTHORITY TO CLASSIFY

1. Top Secret

a. Authority for original classification (article 0231) of information in the Top Secret category is limited to those officials designated hereunder and shall not be delegated except as provided herein.

(1) The Secretary of the Navy; the Under Secretary; each Assistant Secretary; and the Administrative Assistant to the Secretary.

(2) The Chief of Naval Operations; the Vice Chief of Naval Operations; Deputy Chiefs of Naval Operations, Assistant Chiefs of Naval Operations and Directors of Divisions of the Office of the Chief of Naval Operations responsible for the development of strategic and operational plans that meet the requirements for Top Secret classification.

(3) The Commandant of the Marine Corps; Assistant Commandant; Chief of Staff; Deputy Chiefs of Staff, Assistant Chiefs of Staff and Directors of Departments and Divisions of Headquarters, U.S. Marine Corps responsible for the development of strategic and operational plans that meet the requirements for Top Secret classification.

(4) The Chiefs and Deputy Chiefs of the Department of the Navy Technical Bureaus and Offices; and the Chiefs of research and development activities.

(5) Chief, Armed Forces Special Weapons Project (AFSWP) and their deputies, commanders of AFSWP facilities and commanders of commands established by the Joint Chiefs of Staff.

(6) Commanders in Chief; Fleet, Task Force and Type commanders; Commanding Generals of Fleet Marine Forces; and Commander, Military Sea Transportation Service.

(7) Commanders of Naval Sea Frontiers; Commandants of Naval Districts and River Commands; and Commandant of the Marine Corps Schools.

(8) The Commandant of the U. S. Coast Guard and Commandants of Coast Guard Districts when the Coast Guard is operating as part of the Navy.

(9) Other commanders and officials who may be authorized specifically by the Secretary of the Navy.

b. Derivative classification authority (article 0231) for assignment of the Top Secret classification may be exercised by any official whose duties necessitate classifying material created as a result of or in connection with material already classified Top Secret; or when acting on or responding to a communication requiring a Top Secret response.

2. Secret

a. Except as provided herein, authority for original classification of information in the Secret category is limited to the officials designated hereunder:

(1) The officials listed in paragraph 1 above.

(2) Staff officials within the Offices of the Secretary of the Navy, the Under Secretary, the Assistant Secretaries, the Administrative Assistant of the Secretary and the components and activities encompassed by the Executive Office of the Secretary.

(3) Staff officials within the Office of the Chief of Naval Operations and the U. S. Marine Corps Headquarters whose assigned functions and duties include authority to sign documents.

(4) Heads of major staff elements as designated by the Chiefs of the Navy Technical Bureaus and Offices; or by the senior official

of a Naval Shore Establishment Activity acting independently.

(5) Heads of major staff divisions as designated by Chief of AFSWP and Commanders of AFSWP facilities; and heads of major subordinate elements of commands established by the Joint Chiefs of Staff.

(6) Commanders of subordinate fleet, task force or Marine Corps elements and heads of their staff sections; commanders of naval or Marine Corps units on independent missions authorized by major fleet or force commanders.

(7) Heads of activities, components and staff sections designated by Commanders of Naval Sea Frontiers, Commandant of the Marine Corps Schools, Commandants of Naval Districts, MSTS Area Commanders, and Commandants of Coast Guard Districts when the U. S. Coast Guard is operating as part of the Navy.

(8) Naval Attaches and Assistant Naval Attaches.

(9) Heads of independent offices, activities and units (not falling within the scope of 1.a. through 2.a. above) who may be designated specifically by one of the officials listed in 1.a. above.

b. In designating original authority for classification in the Secret category, such designations shall be limited to those officials whose missions and functions demonstrate clearly a necessity for original classification authority for Secret.

c. Derivative classification authority for assignment of the Secret classification may be exercised by any official whose duties necessitate classifying material created as a result of or in connection with material already classified Secret; or when acting on or responding to a communication requiring a Secret response.

3. Confidential

a. Original classification authority to assign the Confidential classification, including Confidential-Modified Handling Authorized, may be delegated by those officials designated in paragraphs 1 and 2 above, who will limit the exercise of this authority as severely as is consistent with the orderly and expeditious transaction of official business.

b. Derivative classification authority for assignment of the Confidential classification may be exercised by any official whose duties necessitate classifying material created as a result of or in connection with material already classified Confidential; or when acting on or responding to a communication requiring a Confidential response.

4. Safeguarding in the Absence of Authority to Classify

a. Nothing in this article shall be construed to relieve originators or signature authorities from the responsibility to provide for adequate safeguarding of official information.

b. When a person originates or transmits material believed to require a classification that he is not authorized to assign, he shall recommend a classification by so marking it, and stating the reason therefore, and refer the material to higher authority.

c. In respect to the foregoing, it is emphasized that, basically, a defense classification marking is merely a signal that the material so marked requires certain minimum controls and restrictions in respect to its accessibility. Should a person have occasion to originate, forward or disseminate material or information that in his best judgement requires a degree of safeguarding equivalent to that prescribed elsewhere in this Instruction for one of the three defense classifications, but who is not designated in this article to have authority to assign such classification, he shall provide adequate controls and precautions commensurate with the importance or sensitivity of such material or information in its handling and transmittal, to ensure against unauthorized or inadvertent disclosure.

5. Safeguarding during drafting or preparation

a. When material is under drafting or preparation for signature or classification by an official who has original classification authority, it is the responsibility of the person drafting or preparing the material to recommend a classification by so marking it in order that notes, discussions, and other pertinent material can be properly safeguarded.

0402. OVERCLASSIFICATION AND UNNECESSARY CLASSIFICATION

1. It is essential that the general public be kept informed as to the programs and policies of the Department of Defense to the maximum extent

permitted by considerations of national security. To accomplish this, unnecessary classification or overclassification must be scrupulously avoided. Information which requires safeguarding shall be assigned the lowest classification consistent therewith.

2. Overclassifying information delays unnecessarily the action on important papers, overburdens security channels and facilities (which results in unnecessary expenditures for costly storage equipment, clearances, document control, etc.), and detracts from the importance of classification in the minds of all personnel. Overclassification undermines our security system and jeopardizes the protection required for important military secrets. In order to assure against overclassification — and conversely to assure proper classification — persons in a command status are responsible for close and continuous supervision of those personnel having classification responsibilities in order to determine the necessity for such authority as well as their competence to assign defense classifications.

0403. STRICT APPLICATION OF CLASSIFICATION CATEGORIES

It is considered that a high proportion of documents have been and are being overclassified, particularly in the Top Secret and Secret categories. It is directed that a strict interpretation of the definitions of these categories, as set forth in Chapter 3, be observed in order to obtain the greatest possible reduction in numbers of such documents.

0404. CLASSIFICATION GUIDES

Each bureau, office, board, agency or activity of the Naval Establishment shall issue a guide for the classification of defense information peculiar to each of their areas of planning, research, technical development (including production) or operation. The examples of classification categories set forth in Chapter 3 provide the basic criteria to be used in the preparation of these guides. The guides shall be kept current by additions or deletions as appropriate.

0405. ADVANCE SECURITY PLANNING

Advance security planning is an essential part of any plan, program, or project wherein security is a major factor. To the extent feasible, each bureau, office, board, agency or activity charged with developing any broad plan, program, or project in which Top Secret or Secret material is involved will insure that arrangements for giving due consideration to security aspects are incorporated therein from the beginning. The basic study or project will include appropriate security guidance, which may be included in a special annex, covering such points as:

1. Issuance of guides for the assignment of classification categories to various portions of the project, as appropriate.
2. Requirements for any special precautions or extraordinary security control measures that need to be observed in order to provide the essential degree of compartmentalization (Circulation Control – Article 0211).
3. Planning for phased downgrading, declassification, and public release of information concerning the project when practicable.

0406. CLASSIFICATION OF INFORMATION ACCORDING TO CONTENT

1. The responsible authority at the time of signature or appoval of any document (and at every opportunity thereafter) shall carefully review its content in the light of the category definition of the classification affixed. In all cases in which security considerations fail to support fully this classification, he shall direct the assignment of a lower classification or declassification. Security considerations shall take into account the ultimate required dissemination of the information involved. In those circumstances where the known necessary dissemination is so extensive that security protection is in fact impracticable, or where effective control must pass substantially from U. S. military authority or other responsible organization, security classifications shall not be assigned or continued.
2. Documents and information, including extracts therefrom, shall be classified according to content and not according to relationship to other classified information.
3. Documents which refer to classified information need not bear the classification of the referenced material provided reference is made by means such as file numbers, dates, other identifying symbols, or subject (provided the subject itself is not classified).
4. Compilations of items of classified information shall be classified in accordance with the definitions set forth in Chapter 3, even though the individual items may separately bear a lower classification than that warranted by the aggregate.

0407. SINGLE CLASSIFICATION

1. Material shall bear the classification of its highest component. Pages, paragraphs, sections, or other components may bear different classifications, but the document or article shall bear only one overall classification.
2. Properly classified Top Secret information shall, whenever possible, be severed from lower classified portions of a document and shall be accorded separate distribution on a considerably more selective and limited basis than the balance of the document.
3. Whenever practicable, material of a lesser classification, which is included in a compilation that has been assigned an overall higher classification, shall be marked with the classification it warrants. This can be accomplished by marking individual paragraphs or sections with the actual classification of material contained therein.
4. A letter of transmittal shall be classified at least as high as the highest classified enclosure but shall, whenever appropriate, be marked for downgrading or declassifying when the enclosure is removed. (Refer to article 0424.)

0408. EQUIPMENT CLASSIFICATION

1. Equipment shall be classified in the same manner as documents and, insofar as is practicable, shall be similarly safeguarded in handling.
2. The responsibility for the initial assignment of classifications to equipment, including components and technical data relating thereto, rests with the chief of the bureau or office under whose direction the equipment was conceived, designed, developed, tested, or procured. However, the Chief of Naval Operations may classify and reclassify equipment.
3. In all cases where bureaus and offices and other Government activities share cognizance or interest in specific equipment, coordination shall be accomplished prior to classifying or reclassifying. The Chief of Naval Operations shall be consulted for a decision if the views of two or more chiefs of bureaus or offices cannot be reconciled.

0409. CLASSIFICATION OF TITLES OR SUBJECTS

Regardless of the overall classification of a classified document, the originator shall assign to it an unclassified title or subject whenever consistent with security and clarity. In all cases, however, the initials of the classification assigned to the title or subject, *standing alone,* will be indicated in parentheses immediately following the title or subject, using one of the following notations: (U), (C), (S), (TS).

For example, the title of a hypothetical Top Secret report might appear on a document as follows: "The First Year's Operations of USS NAUTILUS (U)". This would mean that the title alone of this classified (Top Secret) document is unclassified.

It is not necessary, however, to assign one of the above notations to the subjects of letters, endorsements and memoranda of transmittal if a statement is included thereon in accordance with article 0424 indicating that the document does not itself contain classified information.

0410. CLASSIFICATION OF TITLES OF CIA PUBLICATIONS

The Central Intelligence Agency does not classify separately the titles of its reports and publications but considers that such titles bear the same classification as the reports and publications themselves. Therefore titles of CIA classified reports and publications shall not be used in bibliographies, publications, messages, information reports, distribution lists, indexes, letters, etc., unless the medium in which the title appears bears the same or higher classification as the CIA document itself. Commands desiring to request downgrading or declassification of the title of a classified CIA report or publication will forward such requests to the Chief of Naval Operations (Director of Naval Intelligence), setting forth the purpose for which downgrading or declassification is desired.

0411. CLASSIFICATION OF SHORT TITLES

References by individual short titles to registered documents distributed through the Registered Publications System are unclassified. When three or more short titles of cryptographic publications are listed, a minimum classification of CONFIDENTIAL-MODIFIED HANDLING AUTHORIZED is required. Listings of short titles of noncryptographic publications distributed through the Registered Publications System are unclassified.

0412. CODE WORDS

The current policy and procedure governing the use and classification of code words are contained in OPNAV Instruction 5511.16A and subsequent revisions.

Section 2
CHANGE IN CLASSIFICATION

0413. NEED FOR DOWNGRADING AND DECLASSIFICATION

Overclassification of information causes unnecessary delay and expense in handling and transmission, overburdens stowage facilities, and depreciates the importance of classified information. Under such circumstances, security control is virtually impossible to enforce and to maintain. Therefore, downgrading and declassification shall be accomplished whenever possible.

0414. PROCEDURES FOR RECLASSIFICATION AND DECLASSIFICATION

1. Higher authority in the chain of command or higher authority having primary cognizance over the subject matter involved shall correct an erroneous classification which has been assigned by a subordinate or downgrade or declassify information when such action is deemed appropriate.
2. The originator shall downgrade or declassify, whenever practicable, without reference to other activities, if the subject matter under consideration is entirely within his cognizance.
3. When the interests of two or more commands are involved in the reclassification of information, coordination between such commands is required.
4. When the interests of two or more commands are involved in the reclassification of information and no agreement can be reached, the problem shall be referred for decision, through the chain of command, to the lowest command superior to both.
5. If an originator of classified information no longer exists, the command or activity that has assumed the duties of the originator, or that has primary cognizance over the subject matter involved, shall be responsible for reclassification.
6. In the case of classified information transferred by or pursuant to statute or executive order from another department or agency to the Department of the Navy, for the official use and as part of the official files or property of the Department of the Navy, as distinguished from transfers merely for purposes of storage, the Department of the Navy becomes the classifying authority for all purposes under this Instruction, including declassification and downgrading.
7. When the Department of the Navy has in its possession any classified material which has become five years old, and it appears (a) that such material originated in an agency (outside of the Department of the Navy) which has since become defunct and whose files have not been officially transferred to another department or agency within the meaning of paragraph 6. above, or (b) that it is impossible to identify the originating agency, and (c) a review of the material indicates that it should be downgraded or declassified the Department of the Navy has the power to declassify or downgrade such material. If it appears probable that another department or agency may have a substantial interest in whether the classification of any particular information should be maintained, the power conferred by this paragraph shall not be exercised, except with the consent of the other department or agency, until thirty days after such other department or agency has been notified of the nature of such material and of the intention to downgrade or declassify. During this thirty day period the other department or agency may, if it so desires, express its objections to downgrading or declassifying the particular material, but the power to make the ultimate decision rests in the Department of the Navy. Persons in a command status faced with such a problem should, in case of doubt, refer the problem to higher authority within the Department of the Navy having primary cognizance over the subject matter involved.
8. Activities having a primary interest in and cognizance over the subject matter contained in reports prepared by foreign governments shall recommend to the Director of Naval Intelligence the reclassification of such reports when comparable Navy information is handled in a different security category. The Director of Naval Intelligence shall endeavor to have the originator take appropriate reclassification action.

0415. NOTIFICATION OF CHANGE IN CLASSIFICATION

When information is reclassified, every possible effort shall be made to notify all holders at the time the action is taken.

0416. RECIPIENT TO REQUEST CHANGE

A recipient of information which, in his opinion, is incorrectly classified shall so notify the originator and recommend a change unless such recipient has authority to change the classification on his own responsibility. Such information shall in the meantime be safeguarded in accordance with the recommended or original classification, whichever is higher.

0417. REVIEW BEFORE TRANSFER FOR STOWAGE

Whenever practicable, classified documents shall be reviewed to determine whether or not they can be downgraded or declassified prior to being forwarded to records centers or to the National Archives for stowage. When this is done, certification of classification review shall be affixed to or made on each document sent to stowage, and appropriate changes in classification shall be indicated in accordance with article 0426. When classification review is not considered practicable, a statement to that effect signed by a responsible official shall be attached to each container of classified documents sent to stowage.

0418. DOWNGRADING TECHNICAL EQUIPMENT

Bureaus and offices shall maintain a classification review program for the downgrading and eventual declassification of equipment, including components and technical data relating thereto, as the equipment passes from the stages of initial concept through research, development, test, production, operation, and ultimately to obsolescence and discard (refer to article 0405).

0419. CHANGING SECURITY CLASSIFICATION OF TRAINING FILMS

The procedure for changing security classification of training films shall be the same as for other material. The Bureau of Naval Personnel maintains the security classification records of all Navy training films. All changes must be reported to the Bureau of Naval Personnel for official recording and cataloging. This report shall be identified by the symbol BUPERS 5511.1. Whenever necessary, the Bureau of Naval Personnel shall initiate action to determine whether specific training films may be downgraded or declassified.

Section 3

PREPARATION AND MARKING

0420. PREPARATION OF TOP SECRET

At the time of issuance (signature) of any document which qualifies for assignment to the Top Secret category, the classifying authority shall assure:

1. That unless their retention is required, all preliminary drafts, stenographic notes, and working papers used in preparing the document are destroyed in accordance with disposal regulations contained in chapter 6, section 5 of this Instruction.
2. That all papers of a classified nature which relate to the coordination of the document or other aspects of its preparation and which require retention, including the names of all personnel having had access to the information contained in the document, are itemized, assembled into a single file, and forwarded to the official files of the preparing agency for custody.
3. That each copy of the document is serially numbered as required in article 0607.
4. That each document contains a notation substantially as follows:
   a. "Reproduction of this document in whole or in part is prohibited except with permission of the issuing office or higher authority" (in case higher authority authorizes reproduction, the issuing office shall be notified promptly by such authority. At the time of issuance sufficient copies in anticipation of the need of the recipients should be forwarded).
   b. Where the document itself is Top Secret but portions of it are of a lower classification:
      "Reproduction of paragraph(s) _____* of this document is prohibited except with permission of the issuing office or higher authority" (in case higher authority authorizes reproduction, the issuing office shall be

* Identify such paragraphs as contain Top Secret material.

notified promptly by such authority. At the time of issuance sufficient copies in anticipation of the need of the recipients should be forwarded).

c. When, at the time of issuance, the originator of any document knows that the document or the information contained therein is being furnished for the purpose of compilation or incorporation into a specific plan, study or report:

"Reproduction of this document in whole or in part without permission of the issuing office or higher authority is prohibited, except for the purpose of incorporation into _____."
(Title of plan, study, or report)

5. That each page of the document is numbered as follows:

"page _____ of _____ pages"

0421. GENERAL MARKING

When competent authority specifies that information shall be assigned a classification, such information shall be conspicuously marked "Top Secret," "Secret," or "Confidential," (including Confidential — Modified Handling Authorized) as appropriate, on the original and all copies, as follows:

1. Publications distributed through the Registered Publications System shall be marked in accordance with OPNAV Instruction 2601.7.

2. Classified books, manuscripts, or pamphlets shall be plainly and conspicuously marked "Top Secret," "Secret," or "Confidential" (including Confidential — Modified Handling Authorized) near the top and bottom on all printed pages which contain classified information, on the title page, on index pages (when classified), and on the outside of the front and back covers. Markings shall be well clear of the edges so as not to become covered in assembling or removed by trimming.

3. Classified letters, office memoranda, and other papers which are typed, printed, or written in longhand, and all reproductions thereof, shall be conspicuously marked with the appropriate classification at the top and bottom of each page. The markings shall be placed in a position where they will not become covered in assembling or removed by trimming. When the reverse sides of pages contain classified information, they shall be similarly marked with the classification.

4. Messages shall be marked with an appropriate classification.

5. Classified charts, maps, tracings, photomaps, and drawings shall carry the classification marking adjacent to the legend, title block, or scale in such a manner that the classification is visible if the customary manner of folding is with legend, title block, or scale showing. Classification shall also be marked at the top and bottom in each instance. In addition, where documents may be rolled, classification shall be marked on the reverse side at each end so as to be visible when rolled. Classification markings will be made in such a manner that they will be reproduced on all copies and will be within the margins or borders remaining after trimming.

6. Classified photographs (including all photographic media) shall be conspicuously and appropriately marked with the assigned classification (obverse or reverse). Continuous cover aerial reconnaissance, mapping negatives in roll form, and microfilm of classified records shall be marked with the appropriate classification at the beginning and ending of each roll. These and any other negatives which do not lend themselves to marking shall be safeguarded in the manner prescribed for the assigned classification category, and shall be kept in containers bearing the appropriate classification.

7. Classified motion picture films shall show the classification in the first and last frames and shall be kept in containers bearing the appropriate classification.

8. Classified sound recordings shall be marked with the appropriate classification, if practicable. If marking of a recording is not practicable, its container shall be marked.

9. Original artwork shall have the classification stamped or marked conspicuously on top and bottom margins of the mounting board and on all overlays and cover sheets.

10. All composition tapes shall have the classification stamped at the beginning and ending of each roll and shall be kept in containers bearing the appropriate classification.

11. All reproductions or copies of classified material, regardless of form, shall bear clearly legible classification markings in the same manner as the originals. In this connection it should be noted that office-type copying equipment does not always clearly reproduce all colors of ink or marginal images. Therefore, if the reproduction process

employed does not faithfully reproduce the classification markings appearing on the original copy, personnel engaged in making copies shall mark or stamp the classification on all copies in the same positions and size required for the originals.

0422. SPECIAL EQUIPMENT MARKINGS

The manner of marking classified equipment, products and substances shall depend on the nature thereof. Normally, the assigned classification shall be conspicuously marked by stamping, etching or attaching a classification plate thereto. If this is not possible, the container shall be appropriately marked. If the article or the container cannot be marked, written notification of the assigned classification shall be furnished to recipients of classified equipment, products or substances.

0423. MARKING SIZE AND COLOR

In marking or stamping (not typing alone) the classifications Top Secret, Secret, or Confidential (including Confidential — Modified Handling Authorized), the lettering shall be all capitals and, when practicable, shall be larger than the text of the document and red in color.

0424. MARKING LETTERS OF TRANSMITTAL AND ENDORSEMENTS

1. When the originator of a letter of transmittal or of an endorsement determines that the subject, references, and content of the transmittal or forwarding media do not require the classification of the enclosure or basic material, such transmittal letters and endorsements shall be stamped or marked in a position near the assigned classification with an appropriate phrase, such as the following:

"Downgraded to when enclosure is removed."

"Unclassified when enclosure(s) is(are) removed."

"Downgraded to when basic material is removed."

"Unclassified when basic material is removed."

2. When enclosures are attached to a letter of transmittal or to an endorsement, the entire document shall be accorded the handling required for the highest classification of any enclosure or basic material.

3. When the enclosures or basic material of such a letter of transmittal or endorsement are detached, the transmittal or forwarding media will be handled in accordance with its lower classification.

0425. MARKING FOR AUTOMATIC DOWNGRADING

1. To facilitate downgrading, the originator shall, whenever possible, indicate on the document near the assigned classification the date or event after which the document may be downgraded, as follows:

"Downgraded to Secret on (date, or after specified event)."

"Downgraded to Confidential (or, when appropriate, Confidential — Modified Handling Authorized) on (date, or after specified event)."

"Unclassified on (date, or after specified event)."

2. The above procedure shall not be applied to messages.

0426. MARKING A CHANGE OF CLASSIFICATION

1. When authorized by the originator or higher authority to declassify or reclassify documents, such documents shall be marked as follows:

a. Documents to be upgraded:

Each page of bound or unbound documents which are to be upgraded shall have the old classification marking defaced and the new classification marked or stamped (not typed) thereon, including the front and back covers. The authority for reclassification action shall appear at least on the title page in the case of bound documents and on each page of unbound documents. The notation shall appear substantially as follows:

"Classification (changed to) by

authority of on (date) (signature)."

b. Documents to be downgraded or declassified:

(1) When documents are to be downgraded or declassified a notation substantially as follows shall be marked on the front cover, first page or title page as appropriate by handwriting, stamping, typing or perforating machine:

"Declassified — (authority) — (date) — (unit taking action)"

or

"Secret (or Confidential) — (authority) — (date) — (unit taking action)".

2. Bulk stock of declassified or reclassified documents need not be individually marked until copies are distributed. However, the change in classification shall be indicated on the storage container or inventory control records. At the time of issue, recipients will be given a written notice of reclassification and will be responsible for marking promptly such documents in the manner prescribed in paragraph 1 above.

3. Prints of motion-picture film shall show regrading action on leaders attached between the plain leader and the first frame. Materials such as plates, negatives, standing type, proofs, etc., shall have a statement attached thereto which will show the change in classification but which will in no way alter the reproducibility of the material.

0427. MARKING RESTRICTED DATA

1. A standard classification (Top Secret, Secret, or Confidential) shall be assigned to RESTRICTED DATA. This marking shall be indicated by marking or stamping in the same manner as for other matter. This is in addition to the applicable marking described in paragraph 2 below.

2. The following marking shall be used to identify RESTRICTED DATA:

RESTRICTED DATA
Atomic Energy Act of 1954

The words "RESTRICTED DATA" shall be in lettering larger than the normal lettering which appears on the page and shall be in capital letters.

3. The RESTRICTED DATA marking shall be placed near the marking of the standard classification. However, the RESTRICTED DATA marking need appear only once on each sheet or item containing such matter, preferably at the top.

4. Material which does not lend itself to stamping shall have a metal plate, tag, sticker, or similar device securely attached bearing the standard security classification, as well as the notation required by paragraph 2 above.

5. Classified defense information as defined in article 0305.2 must be identified by the following:

FORMERLY RESTRICTED DATA
Handle as Restricted Data in Foreign Dissemination
Section 144b, Atomic Energy Act, 1954

The above marking shall be placed in the same manner set forth for RESTRICTED DATA in paragraphs 3. and 4. above.

0428. MARKING COMMERCIAL OR INDUSTRIAL PROPRIETARY MATERIAL

Commercial or industrial proprietary information may be identified by the words "Proprietary Information," which shall be written, typewritten, or stamped in capital letters once on each page of information so identified.

0429. MARKING OF CLASSIFIED MATERIAL WHICH IS NOT RELEASABLE TO FOREIGN NATIONALS

1. Whenever the anticipated distribution, transmission, or handling of classified documents is such that the documents will be liable to inadvertent disclosure to foreign nationals, originators or recipients thereof should attach handling notices to the documents, or should incorporate special instructions therein and on the inner envelopes or containers transmitting such documents, as follows:

SPECIAL HANDLING REQUIRED
NOT RELEASABLE TO FOREIGN NATIONALS

When use of this notice is impracticable, as in a message, the abbreviated term "NOFORN" is authorized. This special handling notice normally should be used only on documents furnished for the exclusive use of U. S. military representatives on international staffs or in similar circumstances.

2. In accordance with the provisions of subsection 142d of the Atomic Energy Act of 1954, the Atomic Energy Commission shall remove from the Restricted Data category such data as the Commission and the Department of Defense jointly determine relates primarily to the military utilization of atomic weapons and which the Commission and the Department of Defense jointly determine can be adequately safeguarded as defense information. Provided, however that no such data so removed from the Restricted Data category shall be transmitted or otherwise made available to any nation or regional defense organization, while such data remains defense information except pursuant to an agreement for cooperation entered into in accordance

with subsection 144b, of said Act. Information so removed from the Restricted Data category and safeguarded as defense information shall be marked as follows:

FORMERLY RESTRICTED DATA
Handle as Restricted Data in Foreign Dissemination
Section 144b, Atomic Energy Act, 1954

3. Under no circumstances, however, will classified documents not having a special handling notice attached be released or disclosed to foreign nationals without proper authorization in accordance with policies prescribed in chapter 9, section 4. Special handling notices will be used solely for the purpose of indicating to holders and other handling personnel that the documents involved have already been reviewed by the office of origin or other responsible authority, and that disclosure to foreign nationals is subject to special restrictions.

0430. MARKING OF CLASSIFIED MATERIAL TO BE RELEASED TO FOREIGN GOVERNMENTS

1. Classified documents, including both registered and nonregistered RPS-distributed publications which have been authorized for dissemination to foreign governments or representatives thereof, shall be stamped or marked on the front outside cover of each publication, or there shall be included in the body of the text, if a letter, the following information:

> "This information is furnished upon the condition that it will not be released to another nation without specific authority of the Department of the Navy of the United States; that it will not be used for other than military purposes; that individual or corporate rights originating in the information, whether patented or not, will be respected; and that the information will be provided substantially the same degree of security afforded it by the Department of the Navy of the United States."

2. In addition, if the information is classified Top Secret it shall be stamped or marked with the following statement:

> "This information is released under the condition that a record be kept by the recipient of all individuals who are afforded access to the information contained in the document, and that this record be made available to the Department of Defense of the United States, upon request."

0431. MARKING CLASSIFIED MATERIAL RECEIVED FROM FOREIGN GOVERNMENTS

Defense information of a classified nature furnished to the United States by a foreign government or international organization shall be assigned a classification which will assure a degree of protection equivalent to or greater than that required by the government or international organization which furnished the information.

0432. MARKING RESTRICTED DATA TRANSMITTED OUTSIDE THE DEPARTMENT OF DEFENSE

Documents containing RESTRICTED DATA (Atomic Energy Act), when disseminated to persons outside the Department of Defense or the Atomic Energy Commission, shall be marked as follows:

> "This document contains RESTRICTED DATA within the meaning of the Atomic Energy Act of 1954. Its transmission or revelation of its contents, in any manner not authorized by that Act, is prohibited by law."

0433. MARKING CLASSIFIED MATERIAL DISSEMINATED OUTSIDE THE EXECUTIVE BRANCH OF THE UNITED STATES GOVERNMENT

1. When classified material is furnished authorized persons outside the executive branch of the United States Governnment, the following notation, in addition to the assigned classification marking, shall be placed on the material:

> "This material contains information affecting the national defense of the United States within the meaning of the Espionage Laws, Title 18, U. S. C., Sections 793 and 794, the transmission or revelation of which in any manner to an unauthorized person is prohibited by law."

2. When impracticable to place the above notation on a particular item, it shall be placed on the correspondence notifying the recipient of the classification assigned to the item.

Chapter 5
CONTROL OFFICERS

Section 1
CLASSIFIED MATERIAL CONTROL OFFICERS

0501. DESIGNATION

In order that classified information may be controlled with maximum efficiency, an officer (or in exceptional cases, when an officer is not available, a qualified civilian of comparable grade) shall be designated in each command to serve as the "Classified Material Control Officer." This assignment may be made as regular or additional duty. Assignments of Classified Material Control Officers will be indicated on Form NAVPERS 353, Roster of Officers.

0502. DUTIES

The Classified Material Control Officer shall assist the commanding officer in fulfilling his responsibilities for the security of classified information. To provide most effective assistance, the Classified Material Control Officer shall:

1. Serve as the commanding officer's adviser and direct representative in cases pertaining to the security of classified information.
2. Assure that all persons who are to handle classified information are appropriately instructed and cleared in accordance with this manual.
3. Formulate and coordinate security control measures within the command.
4. Maintain a program of declassification and downgrading of information.
5. Coordinate the preparation of Classification Guides (article 0404) and the development of advance security planning (article 0405) within his area of responsibility.
   a. Assure that all persons who prepare or originate classified material are provided pertinent Classification Guides and are familiar with their use.
6. Exercise security control over visits to and from the command.
7. Initiate action to correct erroneous classifications assigned by subordinates of the command.
8. Maintain records of current classification of information for which the command is responsible.
9. Prepare recommendations regarding release of classified information to foreign governments.
10. Review proposed press releases and indicate classified information which must be deleted therefrom.
11. Perform the duties of Top Secret Control Officer (refer to section 2 below) if a separate officer is not assigned such duty.

Section 2
TOP SECRET CONTROL OFFICERS

0503. DESIGNATION

Persons in a command status who initiate, receive, or process Top Secret documents shall be responsible for the maintenance of a uniform system for handling such documents within their jurisdiction. Commands shall issue additional directives as necessary and shall designate properly cleared subordinate officers or warrant officers (or in exceptional cases, when officers are not available, qualified civilians of comparable grade) as "Top Secret Control Officers" to represent their organiza-

tion in the processing of Top Secret information. The Top Secret Control Officer shall be subordinate to the Classified Material Control Officer.

0504. DUTIES

1. The duties of a Top Secret Control Officer include the receipt, custody, accounting for, and distribution of Top Secret information within the local command, and its transmission outside the command.

2. The following basic directives shall govern the performance of duty on the part of Top Secret Control Officers:

a. Avoid unnecessary dissemination of Top Secret information.

b. Release to a subordinate echelon only the absolute minimum of Top Secret information which is necessary for proper planning or action.

c. Transmit Top Secret information within the command by direct personal contact.

d. Maintain a continuous chain of receipts for all Top Secret information.

Chapter 6
CUSTODY

Section 1
STOWAGE

0601. STOWAGE REQUIREMENTS

1. Classified material not in actual use by appropriately cleared personnel or under their direct personal observation shall be stowed in the manner prescribed in this section.

2. The purpose of this section is to establish physical security standards and requirements which will serve as a uniform guide for determining the kind and degree of physical protection required for classified material.

3. These standards and requirements are designed to provide for flexibility as well as adequacy in the physical security program. More specifically, they are intended to serve the following purposes:

a. Provide a more definite basis for planning and implementation of physical security programs for new activities and evaluating the physical security programs of existing activities.

b. Achieve greater uniformity in the protective measures provided for facilities of like security interest.

c. Achieve greater consistency by narrowing the limits of individual interpretation.

d. Provide a more definite basis for keying security measures to the security interest involved.

0602. NUMERICAL EVALUATION SYSTEM FOR CLASSIFIED MATERIAL IN STOWAGE

1. Purpose.

This method has been developed for the purpose of providing a more specific basis for establishing security protection for material in stowage commensurate with the security interest in such material. It provides not only a means of determining the relationship between the security interest and the level of protection required but also sets forth values for various elements of a security program which may be combined and integrated to produce the required level of protection.

2. Elements of the system.

The elements of the system are as follows:

a. A Table of Numerical Equivalents which establishes numerical values for various items which individually or collectively may be incorporated in the stowage protection program. (Refer to Table A)

b. An Evaluation Graph which establishes minimum levels of required protection based on the classification and the strategic and intrinsic importance of the material concerned. (Refer to Table B)

3. Application of the Numerical Evaluation System.

a. The application of the Numerical Evaluation System to an existing stowage security program is as follows:

(1) Select appropriate numerical equivalents for each applicable element in the security program, as set forth in Table A, the "Table of Numerical Equivalents", and total them. In arriving at such total, it is necessary that a value be assigned for the appropriate element under each of the lettered subsections of Table A and that only one value be assigned under each lettered subsection thereof, with the exception of paragraph 1 of Table A where in cases of concentric containers two items may be selected. It is, of course, permissible to interpolate the values indicated, as necessary to reflect the existing situation.

TABLE OF NUMERICAL EQUIVALENTS

ELEMENT OF SECURITY	VALUE
1. Stowage Container (Two items may be selected where applicable).	
a. None	0
Portable, Any Type	0
Wood, Any Lock	2
Metal, Key Lock	5
Light Room or Building	10
"In Service" ship or MSTS Charter Vessel	10
*Metal, Combination Lock	15
Heavy Room or Building	15
Commissioned Ship	15
*T-20 Safe	20
*Light Vault	20
*X-60, TX-60, or TR-60 Safe	30
*Merchandise Vault	35
*Bank Vault	40
2. **Guarding.	
a. None	0
Civilian Watchman in General Area	5
Civilian Watchman Check of Container every 2 hours	10
Civilian Watchman Check of Container every hour	15
Civilian Watchman Check of Container each ½ hour	20
Civilian Watchman in Attendance at Container	25
Military Guard in General Area	15
Military Guard Check of Container each hour	20
Military Guard Check of Container each ½ hour	25
Military Guard in Attendance at Container	35
b. No Supporting guard force	0
Supporting Guard Force — Civilian	10
Supporting Guard Force — Military	20
c. Aboard Ship in areas where only ship's company have access or visitors are under constant escort	25
3. Protective Alarm System (Refer to Appendix I).	
a. No Alarm on Container	0
System to Detect Opening Container	15
System to Detect Opening or Tampering with Container	20
System to Detect Opening or Tampering with and Approach to Container	30
b. No General Area Alarm	0
System to Detect Entry into General Area	25
4. Control of Personnel Access to Container When Closed or to Contents When Open	
a. System Necessary but not in effect	-20
System not Required	0
System in Effect	5
5. Separately Protected Surrounding Area (Refer to Appendix J).	
a. None	0
Controlled Area, Security Measures	5
Limited Area, Security Measures	10
Exclusion Area, Security Measures	15

*If equipped with so-called "manipulation-resistant" or "manipulation-proof" combination lock, add 5 points.

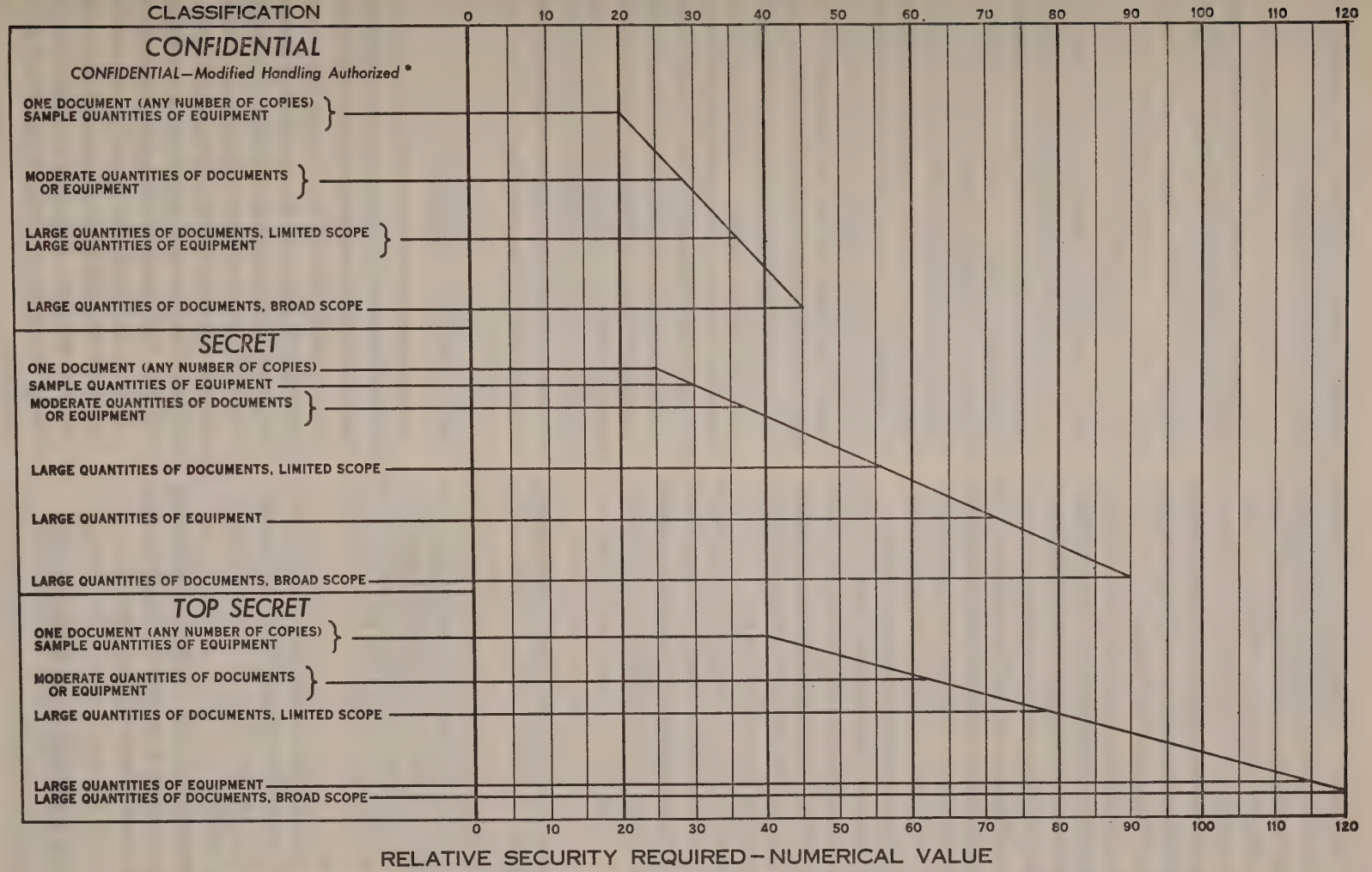
**No value shall be allowed if guards or watchmen assigned to protect United States installations abroad are non-United States citizens. Where policy prevents the use of firearms by guards or watchmen, indicated values shall be reduced by one-half.

(See pages 6-5 — 6-7 for definitions of terms used.)

TABLE A

SECURITY OF MATERIAL IN STORAGE

EVALUATION GRAPH


CLASSIFICATION
0 10 20 30 40 50 60 70 80 90 100 110 120
CONFIDENTIAL
CONFIDENTIAL—Modified Handling Authorized *
ONE DOCUMENT (ANY NUMBER OF COPIES) SAMPLE QUANTITIES OF EQUIPMENT
MODERATE QUANTITIES OF DOCUMENTS OR EQUIPMENT
LARGE QUANTITIES OF DOCUMENTS, LIMITED SCOPE LARGE QUANTITIES OF EQUIPMENT
LARGE QUANTITIES OF DOCUMENTS, BROAD SCOPE
SECRET
ONE DOCUMENT (ANY NUMBER OF COPIES)
SAMPLE QUANTITIES OF EQUIPMENT
MODERATE QUANTITIES OF DOCUMENTS OR EQUIPMENT
LARGE QUANTITIES OF DOCUMENTS, LIMITED SCOPE
LARGE QUANTITIES OF EQUIPMENT
LARGE QUANTITIES OF DOCUMENTS, BROAD SCOPE
TOP SECRET
ONE DOCUMENT (ANY NUMBER OF COPIES) SAMPLE QUANTITIES OF EQUIPMENT
MODERATE QUANTITIES OF DOCUMENTS OR EQUIPMENT
LARGE QUANTITIES OF DOCUMENTS, LIMITED SCOPE
LARGE QUANTITIES OF EQUIPMENT
LARGE QUANTITIES OF DOCUMENTS, BROAD SCOPE
0 10 20 30 40 50 60 70 80 90 100 110 120
RELATIVE SECURITY REQUIRED—NUMERICAL VALUE

* Documents and material designated Confidential-Modified Handling Authorized will normally be stored in the same manner as other Confidential material. When this is not feasible, such documents and material will be stored in a container equipped with a reasonable secure locking device or in any other manner determined by competent authority which will afford adequate protection. This does not preclude a more secure means of storage if desired.

TABLE B

(2) On the left of the graph in Table B, select a subcategory which most accurately describes the material in stowage. Again, it is proper to interpolate. Where the material in stowage is of mixed security interest whether because of classification, scope, or both, the subcategory describing the highest security interest shall be used.

(3) From the subcategory thus selected, proceed horizontally to the point of intersection with the diagonal lines on the graph. The level of protection required, expressed as a numerical value will be found in Table B on the scale at the bottom of the graph directly below the point of intersection. This will reflect the relationship of the existing security program to the standard.

(4) Compare the value obtained in (3), above, to the total of values developed in (1) above. If the security program is below the required standard, the program shall be adjusted to the required level.

b. Similarly, the application of the system to a new stowage situation may be accomplished by determining the level of protection required for the category in which the security interest falls.

0603. STOWAGE REQUIREMENTS FOR CRYPTOGRAPHIC MATERIAL

1. Cryptographic material shall be stowed in accordance with instructions contained in KAG–1A or 2A, except that material requiring cryptographic clearance, irrespective of classification, shall be stowed in the manner prescribed for Top Secret material.

2. Cipher machines (less associated Secret devices) may be stowed in safe lockers which are specially issued for this purpose if a continuous watch or patrol is maintained.

3. Confidential messages marked "Paraphrase Required" (Category B messages) shall be stowed in the manner prescribed for Secret material.

0604. STOWAGE REQUIREMENTS FOR RESTRICTED DATA

1. RESTRICTED DATA shall be stowed in accordance with the stowage requirements for the security classification assigned.

2. The policy concerning security matters and procedures for atomic weapon stowage sites is contained in OPNAV Instruction 05510.25A or subsequent revisions.

0605. KEYS AND COMBINATIONS

It is essential that combinations be known or keys be accessible only to those persons whose official duties demand access to the container involved. The combination or key to a security container shall be changed at the time received, at the time any person having a knowledge of it leaves the organizational unit, at any time there is reason to believe it has been compromised, or in any case not less frequently than every 12 months. Specifying locks with key change rather than hand change combinations will appreciably simplify the task of combination changing. Any paper showing the combination to a lock shall be of the same classification as the aggregate value of material in the container secured by such lock. Records of combinations shall be sealed in an envelope and kept on file by the Classified Material Control Officer, duty officer, communication officer, or other person designated by the commanding officer. In selecting combination numbers, multiples of 5 and simple ascending or descending arithmetical series should be avoided.

0606. CONTAINERS FOUND OPEN

If a container in which classified material is stowed is found unlocked in the absence of assigned personnel, such information shall be reported immediately to the senior duty officer present. The container shall be guarded until the duty officer arrives at the location of the unlocked container. The duty officer shall then inspect the classified material involved, lock the container, and make a security violation report to the commanding officer. If the duty officer believes that classified information may have been compromised, he shall require the responsible person to return to his ship or station to make a definite inspection report. Appropriate further action shall be taken by the commanding officer or higher authority.

DEFINITIONS OF TERMS USED IN THE NUMERICAL SYSTEM FOR THE SECURITY OF CLASSIFIED MATERIAL IN STORAGE ARRANGED IN ORDER OF APPEARANCE IN TABLE OF NUMERICAL EQUIVALENTS

1. Wooden Containers or Light-gage Sheet Metal Containers, Regardless of Type of Lock.
These are looked upon as being of negligible value, except for administrative control in some cases where the container is within a vault or stowage area or is fully protected by an alarm system or continuous guard observation.

2. Steel Filing Cabinets or Desks of the Conventional Office Equipment Type with Key Locks.
Unless such containers are modified by means of steel lockbars and "manipulation-resistant" three-combination dial-type padlock, they offer no appreciable degree of protection. Even so modified, it should be determined that the containers are well constructed and not readily subject to entry by means other than opening the lock before approving them for important stowage.

3. Lightly Constructed Building or Room.
This includes conventional frame or light sheet metal structures; good quality temporary structures, such as temporary warehouses and quonset huts; and ordinary frame and plaster partitioned rooms. They are creditable with full security value for their contents only if all doors, windows, or other sizable openings are either inaccessible, protected by structural means, or secured by good quality "pickproof" locks and cannot be opened from the outside by such means as removing hardware or removing panelled sections.

4. Steel Filing Cabinets with Combination Locks.
This type of container of the conventional ½ to 1 hour fire-resistant type with combination lock offers a good degree of protection against surreptitious entry for a limited time if weaknesses found in some types, which permit opening by means of shims or simple manipulation of the locking mechanism, have been overcome by the proper modifications. This type of container is of little value, however, against a destructive burglarious attack.

5. Heavily Constructed Building or Room.
This includes conventional masonry and steel structures or rooms with better than average partitions, floors, and ceilings. With openings protected as described under Lightly Constructed Buildings or Rooms, they afford a fair degree of security protection against surreptitious entry.

6. Light-weight Steel Safes.
This refers to those safes bearing Underwriters' Laboratories T–20 burglary resisting label. Such safes are considerably more resistant to a burglarious attack than the conventional combination lock filing cabinet, although it must be recognized that they will delay an expert burglarious attack not employing explosives, torches, or power tools only 20 minutes.

7. Light Vaults.
This term applies to the conventional insulated vault with a 3-tumbler combination lock insulated door, with both the vault and the door designed primarily for fire protection. Unless the vault door consists of at least a ⅛" steel plate and is securely fastened in the door opening, and unless the vault walls are of solid masonry (not hollow tile or cinder block) at least eight inches thick, with floor and ceiling of comparable construction, the container should be evaluated as a heavily or lightly constructed room as appropriate.

8. Heavy Steel Safes.
This refers to that group of safes which bear Underwriters' Laboratories labels X–60, TX–60, and TR–60. The labels indicate proven resistance to severe burglarious attempts for a period of 45 minutes and of one hour, including the use of explosives, torches, and power tools.

9. Merchandise Vaults.
This term, adopted from the National Bureau of Casualty and Surety Underwriters, identifies a vault with reinforced concrete floor, walls, and ceiling at least eight inches thick and equipped with a burglar-resistant combination lock door. Merchandise vaults are, for purely insurance purposes, rated by classes A through E, depending upon the type of door used. For the purpose of this standard, doors classed C, D, or E (1", 1½", and 3" of steel respectively) shall be evaluated as Merchandise Vault Doors. They afford a high degree of resistance to burglarious attack.

10. Bank Vaults.

This term, adopted from the National Bureau of Casualty and Surety Underwriters, identifies the most secure types of vaults recognized in insurance rating. Bank vaults have been classified into 10 types, according to their protective capabilities; for each class, both the vault constuction and the door construction are specified. For security purposes, vaults meeting the specifications for Class 6 (18" reinforced concrete walls, 3½" steel door, or specified equivalents), or higher classification shall be evaluated as a Bank Vault.

11. Conventional Combination Locks.

The common 3-tumbler combination lock is constructed in a manner which permits a skilled manipulator through "feel" and sound to determine the setting of the tumblers and, consequently, to open the lock. Depending on the skill of the manipulator, the condition of the lock, and the series of numbers on which the combination was set, successful manipulation of the lock may require from 10 minutes to several hours. However, a skilled manipulator will successfully open the average conventional combination lock in from 15 to 30 minutes.

12. "Manipulation-Proof" or "Manipulation-Resistant" Combination Locks.

"Manipulation-proof" or "manipulation-resistant" refers to a lock so designed that the opening lever does not come in contact with the tumblers until the combination has been set, thereby eliminating the transmission of a revealing "feel" or sound to a manipulator. Such locks furnish a high degree of protection in proportion to their cost and are recommended for containers of highly classified or important material. They may be obtained without any additional cost on new file cabinets, safes, or vaults in some cases.

ADDITIONAL MISCELLANEOUS CONSIDERATIONS.

The following, to varying degrees, affect the protective capabilities of the various types of containers listed above:

1. Size and Weight.

In considering the security of material in stowage, thought must be given to theft of the container as well as its contents. Within security areas where a guard force meeting standards is in attendance, any container weighing in excess of 200 pounds may be considered as not subject to unauthorized removal. In other than guarded security areas, containers smaller than a 4-drawer file cabinet, or lighter than 750 pounds, are not advisable unless securely anchored to the buliding.

2. Locks.

The degree of protection afforded against surreptitious entry into any well-constructed vault, safe, or modern dead-bolt type filing cabinet may normally be measured in terms of resistance afforded by the lock to picking, manipulation, or easily concealable drilling.

a. Key Locks.

The best commercially available key locks can be picked by experts in a few minutes, with the possible exception of certain locks of the type used on safe deposit boxes which require somewhat more time. In addition to its susceptibility to picking, any key lock is a potential weakness in the security system because of:

(1) The possibility of losing the key.

(2) The ease with which an impression may be made of a key.

(3) Difficulty and expense of changing the key every twelve months, or more frequently.

b. Special Combination Locks.

Combination locks with four or more tumblers are commercially available. While each additional tumbler increases the difficulty of successful manipulation, it likewise becomes burdensome to the user. Such locks may be desirable on more important vaults.

c. Lock Drilling.

Practically any lock may be opened by drilling. Usually a very small hole is adequate and usually no apparent damage is done to the lock if drilled by an expert. It is possible to conceal evidence of drilling with reasonable probability of its never being descovered. To overcome this, hardened steel plates may be placed between the lock and the exterior of the container. These can be penetrated by certain drilling techniques, but not without power tools and considerable noise. Safe and

vault doors of better manufacture and rating have "hard plate protection" and should be required for highly important stowage.

3. Relocking Devices.

Relocking devices on safe and vault doors furnish an added degree of protectioin against forcible entry. They appreciably increase the difficulty of opening a combination locked container by means of punching, drilling, or blowing the lock or parts thereof. They are recommended on all heavy safes and vaults.

4. Fire Resistance.

Filing cabinets, safes, and vault doors are very often insulated and bear labels of approval by Underwriters' Laboratories and the Safe Manufacturers National Association as evidence of their proven resistance to certain fire conditions for a given period of time. The fire ratings of these containers or doors do not reflect the protective capabilities of the containers or doors to surreptitious or forcible attack.

Section 2
ACCOUNTING

0607. ACCOUNTING FOR TOP SECRET

1. Except for publications containing a distribution list by copy number, all copies of each Top Secret document and each item of Top Secret equipment shall be serially numbered at time of origination in the following manner:

"Copy No. of copies."

2. The reproduction of all Top Secret documents shall be limited in the manner prescribed in article 0420.4.

3. When Top Secret documents are reproduced with permission of the issuing office or higher authority as per article 0420.4, all reproduced copies shall be serially numbered and immediately recorded with the Top Secret Control Officer so as to maintain complete accountability. A suggested method of identifying the new copies is to label them "copy number 12/1 of_____copies, copy number 12/2 of_____copies, etc.", the first number (12) being the copy number of the original series from which reproduction is being made.

4. Lists of names of all persons having knowledge of a particular item of Top Secret information shall be maintained.

5. A continuous chain of receipts for Top Secret information shall be maintained.

6. The control of all Top Secret information shall be maintained by the Top Secret Control Officer, as prescribed in Chapter 5, Section 2.

0608. ACCOUNTING FOR SECRET

As a minimum requirement, persons in a command status shall establish administrative procedures for recording all Secret material originated and received and shall maintain a receipting system for all Secret material distributed or routed to components of or activities within the command.

0609. ACCOUNTING FOR CONFIDENTIAL

Persons in a command status shall maintain administrative procedures within their commands that will provide accountability for all Confidential information originated or received by the command.

0610. ACCOUNTING FOR PUBLICATIONS DISTRIBUTED THROUGH THE REGISTERED PUBLICATION SYSTEM

In addition to the appropriate accountability requirements set forth in articles 0607, 0608, or 0609 above, publications distributed through the Registered Publication System shall be accounted for in accordance with instructions contained in the effective edition of the Registered Publication Manual.

0611. ACCOUNTABILITY OF CATEGORY B MESSAGES

Unparaphrased copies of classified messages marked "Paraphrase Required" (Category B messages) shall be serially numbered and accounted for through a continuous chain of receipts.

0612. ACCOUNTING FOR TOP SECRET RESTRICTED DATA ORIGINATED BY THE ATOMIC ENERGY COMMISSION

All Navy activities and Navy contractors holding Atomic Energy Commission originated "numbered"

Top Secret documents containing RESTRICTED DATA shall inventory such documents semiannually and shall furnish a copy of the inventory to the Atomic Energy Commission, Central Documents Control Office, 1901 Constitution Avenue, Washington 25, D. C. Such inventories shall be made as of 30 April and 31 October. When no longer required the documents may be destroyed in accordance with the provisions of Section 5 of this chapter; no special report is required by the Atomic Energy Commission, but the destruction must be reflected in the next semi-annual inventory.

Section 3
CUSTODIAL PRECAUTIONS

0613. INDIVIDUAL RESPONSIBILITY

1. All personnel in the Naval Establishment are individually responsible for assuring that knowledge of classified information which they prepare or handle is made available only to persons who have appropriate security clearances and who have clearly established a legitimate "need to know".

2. Personnel of the Naval Establishment shall not remove classified material from the physical confines of the command without the knowledge and approval of the commanding officer or his authorized representative. When classified material is so removed, as when it is taken to conferences or other offices in a local area, a complete list (receipt) shall be prepared, signed by the individual removing the material, and appropriately filed until the material is returned. This procedure is apart from that applicable to personnel in a travel status (see article 0705), to regularly authorized couriers (see article 0710), or to personnel transmitting or routing classified material within Commands or between specifically designated activities (see article 0704).

0614. CARE DURING WORKING HOURS

1. Each individual in the Naval Establishment shall take every precaution to prevent deliberate or casual access to classified information by unauthorized persons. Among the precautions to be followed are:

a. When classified documents are removed from stowage for working purposes they shall be kept face down or covered when not in use.

b. Visitors not authorized access to the particular classified information within a working space shall be received or interviewed in specially arranged reception rooms or areas.

c. Classified information shall not be discussed over the telephone. Telephone scrambling devices do not assure security.

d. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information shall be either (1) destroyed by the person responsible for their production immediately after they have served their purposes, or (2) shall be given the same classification and safeguarded in the same manner as the classified information produced from them.

e. Classified material, upon receipt, shall be opend by the addressee or by persons specifically authorized by him to open material of the grade involved.

2. If, for any reason, a room must be vacated during working hours, the classified material therein must be stowed in the manner prescribed in Section 1 of this chapter and Article 0615.

0615. CARE AFTER WORKING HOURS

1. Commanding officers shall institute a system of security checks at the close of each working day to insure that the classified material held by the command is properly protected. They shall require the custodians of the classified material to make an inspection which shall insure, as a minimum, that:

a. All classified material is stowed in the manner prescribed in Chapter 6, Section 1.

b. All classified material which must be passed from watch to watch is properly accounted for.

c. Burn bags are properly stowed or destroyed.

d. The contents of wastebaskets which contain classified material have been properly stowed or destroyed.

e. Classified shorthand notes, carbon paper, rough drafts, and similar papers have been properly stowed or destroyed. As a matter of routine during the day, such items shall be placed in burn bags immediately after they have served their purpose.

2. Commanding officers shall assure that all personnel concerned are indoctrinated in the requirement for rotating the dial of all combination locks at least three complete turns in the same direction when securing safes, files or cabinets so equipped. In most locks, if the dials are given only a quick twist, it is generally possible to open the lock merely by turning the dial back in the opposite direction. Additionally, responsible personnel shall be required to assure themselves that all drawers of safes and file cabinets are held firmly in the locked position when such equipment has been secured.

3. Commanding officers shall prescribe procedures whereby appropriate identification of the individual responsible for the contents of each container of classified material shall be readily available.

0616. CARE OF WORKING SPACES

In providing for the protection of classified information commanding officers of shore establishments shall:

1. Trim shrubbery outside ground-floor offices to preclude its use as a protective screen for prowlers.

2. Install heavy-duty grilles, screens or bars on ground-floor windows and other accessible openings regardless of location in a building for which credit is taken from Table A of this chapter (see definitions 3 and 5 on page 6–5). Care must be taken to install such equipment by methods which will best serve to defeat access from the outside. In this connection reference to the U. S. Navy Physical Security Manual (OPNAV Instruction 5510.45) is recommended.

3. Take such other precautions necessary to afford protection to buildings and areas in which classified information is kept.

4. Take all practicable precautions to minimize any danger of inadvertent disclosure of classified information in conversations through the use of listening or recording devices. Conference rooms and areas where critical discussions are held are places where extraordinary precautions are necessary:

a. Within the capability of the command, frequent and thorough inspections of such spaces should be made for unauthorized wiring and possible concealment of listening devices in such obvious places as behind pictures, radiators, under desks, etc. (If circumstances warrant, limited professional assistance by trained intelligence personnel is available from the Office of Naval Intelligence, District Intelligence Officers or area Intelligence Officers.)

b. Repairs, routine maintenance and cleaning in sensitive areas should be performed by reliable personnel under supervision.

c. No telephones, office intercommunications or public address systems should be permitted in conference rooms except such amplifier and simultaneous translation facilities as are essential to the conduct of the meeting and unless a technical check can be made before each discussion of classified information.

d. Refrain from discussion of classified information over telephone or intercommunication systems. There is no infallible means of checking for a telephone tap (direct connection or induction).

e. Whenever it is believed that one's conversations are being leaked by some covert means, refer to the suspicion only in temporary written notes, in order that subsequent inspection may then reveal the actual listening device and its origin.

0617. CARE DURING EMERGENCIES

In the event of a fire alarm or other emergency, classified material shall be stowed in the same manner as at the end of a working day. Each person who has classified material in his possession at the time of a fire alarm or other emergency shall assure that such material is properly safeguarded.

Section 4
DISPOSITION OF CLASSIFIED MATERIAL

0618. TRANSFER TO RECORDS CENTERS AND ARCHIVES

Procedures for forwarding documents to Naval Records Management Centers, the National Archives or GSA Federal Records Centers are established by the Secretary of the Navy (Administrative Officer). Classified documents so forwarded shall be safeguarded in accordance with the regulations set forth in this manual. The procedures for the transfer of records apply to record material as defined in SECNAV Instruction 5212.5 or subsequent revisions. Extra copies and non-record material shall be destroyed after their period of usefulness has ended.

0619. DISPOSITION OF CLASSIFIED MATERIAL BY PERSONS RELEASED OR SEPARATED FROM THE NAVAL ESTABLISHMENT

1. When military or civilian personnel resign or are to be separated from the Naval Establishment or released from active duty, all classified material held by them shall be turned in to the source from which received, to their commanding officer, or to the nearest naval command, as appropriate, prior to the delivery of final orders or separation papers.
2. Military or civilian personnel to resign or to be separated from the Naval Establishment or to be released to inactive duty shall submit to their commanding officer a signed statement which contains the following:

a. Certification of compliance with 1. above.

b. Certification that they understand that they are not to reveal classified information of which they may have knowledge unless officially directed in writing to do so by competent naval authority.

c. Certification that they have read and understand appendices B, D, E, F, and H of this Instruction.

These statements shall be executed prior to the delivery of final papers. In the case of military personnel the statements shall be made part of the official records of the personnel concerned; statements of civilian personnel will be retained in command records for two years. (Refer to appendix A for Security Termination Statement.)

0620. TRANSFER ON RELIEF

An officer about to be relieved shall deliver to his successor all classified material attached to the command and within his custody. Appropriate receipts shall be completed covering as a minimum all Top Secret and Secret material.

0621. RECOVERY ON DEATH OR DESERTION

Upon the death or desertion of a person in the Naval Establishment, or when any person is declared "missing in action" or "missing", the commanding officer, in disposing of the personal effects of such person shall insure that those effects contain no classified material. Every endeavor shall be made to recover classified material known to have been in the possession of such person.

0622. AVOIDING ACCUMULATIONS OF CLASSIFIED MATERIAL

Classified material not required by a naval command shall not be allowed to accumulate but shall either be destroyed in accordance with section 5 of this chapter or be sent to stowage at a Naval Records Management Center or other official records depository.

Section 5
DESTRUCTION OF CLASSIFIED MATERIAL

0623. DESTRUCTION OF CLASSIFIED DOCUMENTS

Destruction of (a) classified records so authorized by Record Disposal Schedules, (b) nonrecord classified documents as defined in SECNAV Instruction 5212.5 or subsequent revisions, or (c) classified waste material shall be made by one of the following methods:

1. Top Secret, Secret, or Confidential documents; registered publications; or any classified messages shall be destroyed by burning except as provided in paragraph 2 below.

a. Burning shall be accomplished in the presence of two witnessing commissioned officers. If commissioned officers are not readily available at an activity warrant officers, enlisted personnel or civilian employees may perform the duties of witnessing officers. All persons witnessing the destruction of classified material must have security clearances at least as high as the category of material being destroyed.

b. When appropriate, certificates of destruction shall be prepared and signed by the witnessing officers. (Refer to article 0625.)

c. Witnessing officers shall watch the burning until the classified documents are completely consumed. Oil or chemicals to facilitate burning may be used.

d. Residue shall be completely obliterated by such methods as scattering or reduction to sludge.

e. Portions of burning material must be prevented from being carried away by wind or draft.

2. Top Secret, Secret and Confidential documents may be destroyed by pulping provided destruction of the classified material is complete and reconstruction is impossible.

0624. DESTRUCTION OF EQUIPMENT

When it is necessary to dispose of equipment that still must bear a security classification, destruction shall be accomplished by any means that will prevent recognition and reconstruction. Jettisoning of classified equipment in water of sufficient depth to preclude any possibility of recovery may also be employed.

0625. RECORDS OF DESTRUCTION

1. An accurate record of destruction of classified material is as important as its destruction. Proper accounting procedures, together with accurate records of destruction, provide official information as to the status of highly classified material.

2. A Certificate of Destruction of nonregistered Top Secret and Secret documents shall be prepared. The certificate shall be retained for a period of 2 years by the command destroying the material. The certificate shall provide complete identification of the material destroyed, the date of destruction, and it shall be signed by the officer authorizing destruction. In the case of non-registered Secret documents only, use of routing sheets, mail logs, or other similar administrative records in lieu of a Certificate of Destruction is authorized, *provided* that all necessary information (complete identification of the material destroyed, date of destruction, signatures of officer authorizing destruction and of witnessing officers) is included thereon.

3. Certificates of destruction shall be prepared for all classified equipment destroyed. The certificate shall be retained for a period of 2 years by the command destroying the equipment, and a copy of the certificate shall be forwarded to the technical bureau or office responsible for procurement of the equipment.

0626. DESTRUCTION OF REGISTERED PUBLICATIONS AND COMMUNICATION EQUIPMENT

Registered Publications and many types of communication equipment carry special destruction instructions. Refer to the appropriate instruction prior to destroying any Registered Publication or communication equipment.

0627. EMERGENCY DESTRUCTION

In an emergency involving the danger of capture of classified material, the importance of beginning its destruction sufficiently early cannot be overemphasized. The consequences of such destruction which may be determined, as a matter of hindsight, to have been unnecessary, may be relatively unimportant when measured against their compromise through capture. Destruction plans of particular activities, therefore, will call for the exercise, by personnel at all levels, of the highest degree of individual initiative practicable under the operating conditions of such activity, in preparing for and in actually commencing destruction required under the plan. Particular care will be taken to indoctrinate all personnel to insure their understanding that, in such emergencies and when required, they will initiate necessary destruction under the plan without waiting for specific orders. Lists shall be prepared which show the locations of classified material, personnel responsible for destruction, and the recommended place and method of destruction.

0628. PRIORITY FOR EMERGENCY DESTRUCTION

1. Communication Material. Insofar as humanly possible, cryptomaterial shall not be permitted to fall into enemy hands. In general, emergency destruction of communication material shall be carried out as follows:

a. *First Priority — Cryptographic material. (Detailed information concerning the order of destruction of cryptomaterial is contained in KAG-1, KAG-2 and RPS 4).*

b. *Second Priority — Noncryptographic material distributed by the RPS in the order of classification: highest classified material first.*

2. Other Classified Material. Emergency destruction of other classified material shall be carried out in order of priority as follows:

a. Material pertaining to current and future plans and operations.

b. Material pertaining to standing operating or tactical procedures.

c. Equipment of a classified nature together with pertinent technical descriptive and operating instructions.

d. Remaining classified material. The order of destruction will follow classification, the highest classified material will be destroyed first.

0629. ACCESSIBILITY FOR DESTRUCTION

1. Classified material shall be readily accessible at all times for destruction by assigned personnel. As practicable, publications on board ships shall be stowed in weighted, perforated canvas bags or weighted binders which are of a size to allow ready access to publications for use and to permit ready handling by one or two men when emergency destruction by jettisoning is necessary.

2. Material to be destroyed first shall, when practicable, be marked in a distinctive manner and stowed in the most accessible location.

3. Keys and safe combinations to spaces where classified material is stored may be kept in selected locations, safeguarded by proper security arrangements.

Chapter 7
TRANSMISSION

Section 1
METHODS OF TRANSMISSION

0701. TRANSMISSION OF TOP SECRET MATERIAL WITHIN THE CONTINENTAL UNITED STATES

1. Top Secret material shall be transmitted by one of the following means:
   a. Direct personal contact of officials concerned.
   b. Armed Forces Courier Service.
   c. Electric means in encrypted form.
2. Top Secret material shall not be transmitted through the United States postal system or any foreign postal system.

0702. TRANSMISSION OF SECRET AND CONFIDENTIAL MATERIAL WITHIN THE CONTINENTAL UNITED STATES

1. Secret and Confidential material shall be transmitted by one of the following means:
   a. Any of the means approved for the transmission of Top Secret material.
   b. U. S. Registered mail.
2. Confidential — Modified Handling Authorized may be transmitted by ordinary U. S. mail or electrically in unencrypted form over U. S. Government owned or leased land lines. When the originator is uncertain of the location of an addressee, as in the case of an afloat unit, U. S. registered mail shall be used.
3. Refer to article 1304 for instructions for mailing messages classified Secret and Confidential.

0703. TRANSMISSION OF CLASSIFIED MATERIAL OUTSIDE THE CONTINENTAL LIMITS OF THE UNITED STATES

1. Classified material shall not be transmitted by mail, express, courier, pouch, electric means, or any other system of transmission operated or controlled by a foreign government except as provided in 2. f. and g. below.
2. Authorized methods for the transmittal of classified material outside the continental limits of the United States are:
   a. Direct personal contact of officials concerned.
   b. Electric means in encrypted form.
   c. Armed Forces Courier Service.
   d. Accompanied diplomatic pouch.
   e. By US Registered Mail in US Military postal channel, for Secret and Confidential only. (See OPNAV INST. 2720.10A or subsequent revisions.)
   f. Registered mail with Registered mail receipt between United States Government and/or Canadian Government installations in the continental United States, Canada, or Alaska for Secret and Confidential material only.
   g. Confidential — Modified Handling Authorized may be transmitted by ordinary first class mail which is under the control of the United States or Canadian Governments, or transmitted by unaccompanied State Department air or surface pouch under diplomatic seal.

0704. TRANSMISSION WITHIN COMMANDS OR BETWEEN SPECIFICALLY DESIGNATED ACTIVITIES

1. Notwithstanding the requirements for the formal transmission of classified material as prescribed in articles 0701 through 0703, commanding officers are authorized to establish systems for the transmission of classified material within the local confines of their commands or activities and between specifically designated activities.
2. Transmission systems established by individual commands shall operate to assure that—
   a. Top Secret material is always controlled by Top Secret Control Officers;

b. Top Secret material is transmitted only by commissioned officers or warrant officers or responsible officials of comparable grade who have been granted Top Secret security clearances;

c. Personnel transmitting Secret or Confidential material have security clearances of a category at least as high as the material being transmitted;

d. Personnel (officer, enlisted, or civilian), whose primary duties involve the transmission of classified material, are specifically designated in writing as being authorized by the command for such duties; and all classified material being transported is protected from casual observation;

e. All persons entrusted with the transmission of classified material are instructed in the proper procedure for safeguarding the material being transmitted.

0705. PROTECTION OF CLASSIFIED MATERIAL BY PERSONNEL IN A TRAVEL STATUS

When persons within the Naval Establishment or Navy contractors are required to travel in the performance of their official duties and when classified material is involved in connection with such duties, the following procedures shall apply:

1. A determination shall be made to ascertain whether the necessary classified material is available at the destination of the traveler. If the material is available, no additional transmission shall be authorized.

2. If the needed classified material is not available at the destination of the traveler, commanding officers shall, whenever possible, have the classified material transmitted to the activity being visited in accordance with articles 0701 through 0704, as appropriate.

3. If it is impossible to comply with either paragraph 1 or 2 above, commanding officers may authorize appropriately cleared personnel to carry or transmit classified material on their persons between their duty station and the activity to be visited, subject to the following conditions:

a. The classified material shall be in the physical possession of the individual at all times if proper stowage at a U. S. Government activity or appropriately cleared contractor facility (continental U. S. only) is not available. Classified material shall not be left in such places as locked automobiles, hotel rooms, hotel safes, train compartments, private residences, public lockers, etc.

b. Classified material shall not be read, studied, displayed, or used in any manner in public conveyances or places.

c. Written statements authorizing the transmission or carrying of classified material shall be provided by commanding officers to all individuals traveling outside the continental United States. This authorization statement, together with official travel orders, should ordinarily permit the individual to pass through any customs without the need for subjecting the classified material to inspection. If difficulty is encountered, the individual should refuse to disclose the classified material to customs inspection and should insist upon the assistance of the local U. S. military or State Department representatives at the port of entry or departure.

d. A list of all classified material carried or transmitted by individuals traveling will be maintained by the command to which the individual is attached. Upon return of the traveler, all classified material shall be accounted for.

e. All individuals authorized to carry or transmit classified material while in a travel status shall be fully informed of the provisions of this article prior to departure from their duty station.

0706. TRANSMISSION OF RESTRICTED DATA

RESTRICTED DATA shall be transmitted in the same manner as other material of the same security classifications.

0707. TRANSMISSION OF CRYPTOGRAPHIC AND REGISTERED MATERIAL

Prior to the transmission of cryptographic and registered material, commanding officers shall refer to communication instructions and the Registered Publication Manual for detailed procedures.

0708. TRANSMISSION OF BULKY MATERIAL

1. *Government Carrier.* When an item of classified material cannot be transmitted in accordance with the provisions of articles 0701 through 0707

because of size and weight, Government vehicles, aircraft or ships operated by appropriately cleared personnel, including necessary guards, will meet the requirements for safeguarding classified material. (See articles 0704 and 0705 for necessary precautions).

2. *Commercial Carrier.* When shipment by military owned and operated transportation facilities is not feasible, commanding officers shall protect shipments made by commercial transportation facilities by every means at their disposal. Whenever commercial transportation facilities are utilized for the shipment of classified material, commanding officers shall:

a. Package all classified material in containers in a manner that shall prevent the observation of the contents thereof by unauthorized persons and shall reveal attempts to gain access thereto.

b. Assure that bills of lading do not contain classified information or details that would make obvious the classified nature of the shipment.

c. Notify consignees and transshipping activities by separate correspondence of all classified shipments. Such correspondence shall be tansmitted by means which will assure that the consignees and transshipment activities are advised of the shipments in advance of their arrival.

d. Assure that classified blueprints, manufacturing drawings, etc. are not shipped in the same package with the classified equipment. This is not intended to prevent the enclosure of essential operating, installation, or maintenance instructions, and the usual inventory lists, which are normally included in equipment shipments.

3. Subject to the foregoing, commercial shipments of classified material shall meet the minimum requirements as follows:

MINIMUM REQUIREMENTS TO BE USED IN THE TRANSPORTATION OF CLASSIFIED MATERIAL

WITHIN CONTINENTAL UNITED STATES

Type of Carrier	Top Secret	Secret	Confidential (Confidential Modified Handling Authorized)
Air Express	NA	NA	(Including Canada & Alaska) NA
Railway Express	NA	G or H	G, H or L
Less than Truck Load	A	C or J	J or L
Truck Load	A	C or J	F
Less than Carload	NA	NA	L
Carload	A	B	E
Airfreight	A	J	I
Forwarders (Air & Surface)	NA	NA	NA

OUTSIDE CONTINENTAL UNITED STATES

Type of Carrier	Top Secret	Secret	Confidential (Confidential Modified Handling Authorized)
MSTS, GAA	A	D	J or K
MSTS, USNS	A	D	J or K
Commercial U. S. Flag Vessels	A	D	J or K
Foreign Flag Ships or Aircraft	NA	NA	NA
Airfreight (U. S. Flag Carriers)	A	D	J
Forwarders (Air & Surface)	NA	NA	NA

A. Under the continuous protection of military guards, one of which must be a commissioned or warrant officer of the U. S. Armed Services and cleared for access to Top Secret material.

B. Car or cars of sufficient capacity to transport the material should be ordered from the rail carrier. The material must be under the continuous protection of either civil service, civilian contractor or military escorts, one of which will be cleared for access to Secret material. Closed cars will be used unless the nature of the material precludes use of closed equipment. If closed equipment cannot be used, the material will be completely covered by tarpaulins or other suitable covering material, so secured as to reveal attempts to gain access thereto. Closed cars will be sealed by the use of Navy Seals which will not be broken in transit by unauthorized persons.

C. Exclusive use of the transporting equipment must be obtained. The material must be under the continuous protection of either civil service, civilian contractor or military escorts, one of which will be cleared for access to Secret material. Closed motor vehicles will be used unless the nature of the material precludes use of closed equipment. If closed equipment cannot be used, the material will be completely covered by tarpaulins or other suitable covering material, so secured as to reveal attempts to gain access thereto. Closed motor vehicles will be sealed by the use of Navy Seals which will not be broken in transit by unauthorized persons.

D. Under the continuous protection of military guards, one of which will be cleared for access to Secret material. Material shall be, if practicable, stowed in such a manner as to be under the surveillance of guards at all times.

E. Car or cars of sufficient capacity to transport the material should be ordered from the rail carrier. Closed cars will be used unless the nature of the material precludes use of closed equipment. If closed equipment cannot be used, the material will be completely covered by tarpaulins or other suitable covering material, so secured as to reveal attempts to gain access thereto. Closed cars will be sealed by the use of Navy Seals which will not be broken in transit by unauthorized persons.

F. Exclusive use of the transporting equipment must be obtained. Closed motor vehicles will be used unless the nature of the material precludes use of closed equipment. If closed equipment cannot be used, the material will be completely covered by tarpaulins or other suitable covering material, so secured as to reveal attempts to gain access thereto. Closed motor vehicles will be sealed by the use of Navy Seals which will not be broken in transit by unauthorized persons.

G. In "Armed Surveillance Service". (Carload lots of confidential material may be shipped as provided in E without the requirement for armed surveillance.)

H. In "Armed Guard Service". (Use of this service must be authorized by Bureau of Supplies and Accounts, Code H2).

I. In "Signature Service" provided provision has been made therefor in currently effective tariffs.

J. When escorted by either military, civil service personnel or civilian contractor personnel, cleared for the level of security of the material escorted.

K. Use of the standard Navy metal cargo "unit load shipping container" or similar metal container is authorized when a Navy Seal and a padlock or combination lock are applied. The seals shall not be broken in transit by unauthorized persons.

L. When weight of material plus container is not less than 200 pounds; and

a. Packaged in secure metal containers so secured with Navy numbered seals as to prevent access unless a seal is broken, or

b. Packaged in wood cleated plywood, or wood cleated paper overlaid veneer conforming to Federal Specifications PPP–B–601a (Style B). Such boxes will be of previously unused or new construction and shall be closed and strapped in accordance with the appendix to the Specifications.

NA. Not authorized.

4. Excessively bulky equipment constructed into one piece, concealed internal parts of which are classified, need not be shipped as classified material provided that scrutiny of the exterior profile of the equipment will not reveal classified information and that such equipment must be taken apart in order to gain access to the classified material.

5. Bulky equipment, small removable parts of which are classified, will if practical have the classified parts removed and packed in accordance with its classification and shipped separately. The unclassified portion will then be shipped as unclassified material. In such cases shipping officers will be responsible for preparing and distributing notification of separate shipment and documentation covering.

6. Military guards, when required, shall be provided by the naval command originating the shipment. If a security force is not under the operational control of the originating naval command the commandant of the naval district or river command or area naval commander in which the shipment originates shall provide the guards. The arming of military guards will be at the discretion of the naval command originating the shipment. Military aircraft officers or ships' officers of fleet or Military Sea Transportation Service vessels, who are cleared to the level of the defense classification of the cargo to be transported, may be used in lieu of military guards.

7. The Navy Shipping Guide, Part I, will be referred to for a detailed explanation of the transportation services described above.

Section 2

TRANSMISSION BY COURIER

0709. ARMED FORCES COURIER SERVICE

1. The Armed Forces Courier Service, established by action of the Joint Chiefs of Staff on 9 January 1953, is a joint agency of the Departments of the Army, Navy, and Air Force to provide for the secure and expeditious transmission of material requiring protected handling by officer courier. Security is the paramount objective of the Armed Forces Courier Service and speed will be sacrificed at any time in order to achieve that objective. Courier service

shall be performed impartially by the three services for all services in the interest of economy and efficiency. The development and promulgation of policy and regulations affecting or providing for the transmission of classified material is the responsibility of the Secretaries of the Military Departments. Detailed instructions are set forth in OPNAV Instruction 2260.1A (or subsequent revisions), Armed Forces Courier Service Regulations.

2. The following types of material are authorized for entry into the Armed Forces Courier Service:

a. Top Secret material.

b. Qualified cryptographic material.

c. Qualified cryptologic material.

d. Qualified Registered Publications System material.

e. Communication material, which cannot be transmitted electronically because of circuit outage, and certified by a Commanding Officer as official business requiring urgency of the highest priority with respect to transmission.

f. Such other material as may be specifically approved by the Chief of Staff, U. S. Army; the Chief of Naval Operations; and the Chief of Staff, U. S. Air Force.

g. Any U. S. official material in transit, the control over which cannot be maintained in U. S. custody by any means other than an officer courier.

h. State Department diplomatic courier pouches.

i. Qualified material of the Central Intelligence Agency.

j. Qualified material of the National Security Agency.

k. Material, as defined in a. through g. above, of the North Atlantic Treaty Organization destined for transmission between the Standing Group, Supreme Headquarters Allied Powers in Europe, NATO Military Units within the areas served by ARFCOS Courier Transfer Stations, and the U. S. Government.

Section 3

PREPARATION OF MATERIAL FOR TRANSMISSION

0710. CONTAINERS

1. Whenever material classified Top Secret, Secret or Confidential is transmitted by the Armed Forces Courier Service, diplomatic pouch, registered U. S. mail, registered Canadian mail, or nonregistered U. S. mail, as provided in article 0701 through 0705, it shall be enclosed in two opaque sealed containers (wrappings or envelopes), except that material designated as Confidential — Modified Handling Authorized may be enclosed in a single container.

a. Classified written material shall be folded or packed in such manner that the text will not be in direct contact with the inner container. A receipt form shall be attached to or enclosed in the inner container, except that material classified Confidential shall require a receipt only if the originator deems it necessary.

b. The inner container shall show the address, classification, including where appropriate the "RESTRICTED DATA" marking, and any applicable special instructions. It shall be carefully sealed so as to minimize the possibility of access without leaving evidence of tampering.

c. An outer or single container shall show the complete and correct address and the return address of the sender.

d. An outer cover or single container shall not bear a classification marking, a listing of the contents divulging classified information, or any other unusual data or marks which might invite special attention; except that classified material prepared for transmission by the Armed Forces Courier Service or State Department accompanied diplomatic pouch shall be prepared with a single container with the classification plainly marked thereon. (ARFCOS and State Department accompanied diplomatic pouches are considered to be the outer covers for such material.)

2. To minimize the possibility of compromise of classified material caused by improper or inadequate packaging thereof, commanding officers will ensure that proper wrappings are used for mailing bulky packages. Commands should provide for the stocking of several sizes of cardboard containers, corrugated paper and kraft tape laminated with asphalt and containing rayon fibers (snake tape) or nylon

sensitive tape. Commanding officers shall require the inspection of bulky packages to determine whether the material is suitable for mailing or whether it should be transmitted by other approved means.

3. In order to minimize the damage to the defense interest of the United States resulting from the loss of or unauthorized access to classified equipment in shipment, such documents as design blueprints and manufacturing drawings shall be shipped under separate cover unless competent authority determines that the needs of the service would be unduly jeopardized thereby.

0711. ADDRESSES

Except in unusual circumstances approved by competent authority, classified material shall be addressed to recognized activities and not to individuals. This is not intended, however, to prevent use of office code numbers or such phrases in the address as "Attention: Research Department", or similar aids in expediting internal routing, in addition to the oganization address.

1. The following publications shall be consulted for complete and correct mail addresses and mailing instructions.

   a. Current issues of the Standard Navy Distribution List, Part 1, contain the official list of fleet and mobile units and their administrative addresses.

   b. Current issues of the Catalog of Naval Shore Activities including Standard Navy Distribution List, Part 2, contain the official list of shore activities with complete administrative addresses.

2. Care must be taken to ensure that classified material intended only for the United States elements of international staffs or other organizations is addressed specifically to those elements.

3. During wartime, naval addresses shall meet joint Army, Navy, and Air Force security requirements by not disclosing a geographical location except on Armed Forces Courier mail. Upon the outbreak of war or when ordered, naval activities outside of the United States shall use the numerical and mobile mail addresses as prescribed by the Chief of Naval Operations, unless otherwise specifically directed.

0712. RECEIPT SYSTEMS

1. Top Secret material shall be transmitted under a continuous chain of receipts.

2. Secret material shall be covered by a receipt between commands and other authorized addresses and, as a minimum requirement, between components of or activities within the command.

3. Receipts for Confidential material may be required at the discretion of the transmitter.

4. Receipt shall be provided by the transmitter of the material and the forms shall be attached to or enclosed in the inner cover.

   a. Post-card receipt forms shall be used whenever practicable.

   b. Receipt forms shall be unclassified and contain only such information as is necessary to identify the material being transmitted.

   c. Receipts shall be retained for at least 2 years.

5. Receipts for publications distributed through the Registered Publication System shall be handled in accordance with the Registered Publication Manual.

Chapter 8
SECURITY VIOLATIONS AND COMPROMISES

0801. REPORT OF LOSS OR COMPROMISE

1. Any person in the Naval Establishment having knowledge of the loss or possible subjection to compromise of classified information shall report the facts immediately to the most readily available command, who, following preliminary inquiry, shall:

a. Report immediately the loss or possible subjection to compromise to the command having custodial responsibility for the information by appropriate rapid means, forwarding an information copy of the report to the originator* of the information.

b. Make (or arrange for) a thorough inquiry or investigation of the circumstances. The inquiry shall include statements of all persons concerned, and, whenever possible, a determination of the individual or individuals responsible. If the circumstances indicate, he may request the services of Naval Intelligence in accordance with the provisions of SECNAV Instruction 5430.13A or subsequent revisions.

c. Forward, as soon as practical, the report of the inquiry or investigation of the loss or possible subjection to compromise to the command having custodial responsibility for the classified information; the latter shall include therein an account of the disciplinary or corrective action taken and forward the complete report to the originator* of the information, with copies to:

(1) The Chief of Naval Operations (Director of Naval Intelligence) via the administrative chain of command in all cases.

(2) The Chief of Naval Material, for losses or possible subjections to compromise occurring within industrial concerns.

2. In addition to the requirements set forth in paragraph 1 above, whenever loss or possible subjection to compromise occurs in the case of RESTRICTED DATA, the nearest District Intelligence Office (or, in the case of commands located outside the U. S., the Office of Naval Intelligence) shall be notified immediately so that this information may be passed to the Federal Bureau of Investigation.

3. Whenever loss or possible subjection to compromise occurs in the case of cryptographic material or registered publications or devices, the following action shall be taken *in place of* the requirements set forth in paragraph 1 above and in accordance with applicable instructions (Refer to OPNAV INST 2221.2 series):

a. In the case of cryptographic material, a report by message shall be made to the Director, National Security Agency (DIRNSA) and the Chief of Naval Operations.

b. In the case of registered publications and devices, a report shall be made either in accordance with 0801.3.a. above or directly to the Chief of Naval Operations, as appropriate.

4. When classified material is received, the outer covering of which is in damaged condition or shows evidence of having been repaired, so there is a possibility of compromise, Commanding Officers shall submit a report of the damage to the originator and to the delivering activity. Such reports do not preclude or take the place of the report required by paragraphs 1 and 3 above; they shall in any case always include pertinent comment as to the preparation of the classified material for transmission to assist the originator in determining whether violations of article 0710.1.a. have occurred.

0802. SABOTAGE OR ESPIONAGE

Individuals becoming aware of possible acts of sabotage, espionage or other subversive activities shall

* When the originator is not a Navy or Marine Corps command or activity, notification shall be made via the Chief of Naval Operations.

report immediately all available information to the most readily available command who in turn shall notify immediately the Director of Naval Intelligence or the cognizant Naval District Intelligence Officer, as appropriate.

0303. EVIDENCE OF TAMPERING WITH COURIER MAIL

Any evidence of tampering with Courier Mail shall be reported immediately by message to the Director, Armed Forces Courier Service, to the Chief of Naval Operations (Director of Naval Intelligence), and to the originator.

0304. SECURITY VIOLATIONS

1. Violations of regulations pertaining to the safeguarding of classified information, but not resulting in its loss, compromise, or unauthorized disclosure, shall be acted upon by the commanding officers of the persons involved without reference to other authority. The fact that a breach of security regulations has occurred may, in the discretion of the commanding officer, be considered as sufficient jusification for some form of disciplinary action, whether or not there has been a loss or possible subjection to compromise. The circumstances of the case, including the degree of culpability, should always be considered in determining when disciplinary action is appropriate.

2. Persons in command status shall establish such measures for the security inspection of safe-stowage containers and of areas where classified material is maintained as are necessary to assure compliance with security regulations.

3. Persons in command status who receive classified material which shows improper handling by the activity from which received will promptly advise the commanding officer of that activity.

0305. DISCIPLINARY ACTION

Individuals found responsible for the loss, unauthorized disclosure or possible subjection to compromise of classified information, and individuals who violate security regulations, shall be promptly and adequately disciplined regardless of rank or position. Even where it is impossible to identify the specific individual source of an unauthorized disclosure of classified information, disciplinary action is not necessarily precluded. Where the source can be traced to a specific command or office, the commander or official in charge shall be held responsible for any derelictions or ineffectiveness in the discharge of his responsibilities in such manner as may be warranted in the circumstances. Disciplinary action may include, in the case of military personnel, trial by court-martial or, in the case of civilians, processing under the Standard Schedule of Disciplinary Offenses and Penalties for Civilian Employees in the Naval Establishment included in NCPI 45, prosecution under title 18, U.S.C., as amended, or other Federal statutes as appropriate. Offenses by civilian employees of the Navy shall be reviewed for applicability of the Act of 26 August 1950 (5 U.S.C. 22–1 et seq.) and Executive Order 10450 as amended pertaining to security risks. (Refer to appendices C and G).

Chapter 9
CONTROL OF DISSEMINATION

Section 1
GENERAL

0901. RESPONSIBILITY

1. Persons in a command status shall be responsible for controlling the dissemination of classified information emanating from or distributed within their commands. They shall also be responsible for the promulgation of additional directives that may be required to prevent unauthorized dissemination of information under their control.
2. The existence, nature, content, or whereabouts of classified information shall not be divulged needlessly.
3. No person is entitled to knowledge or possession of classified information solely by virtue of his rank, office, or position.
4. Classified material shall not be removed from a command without the specific permission of the commanding officer or his authorized representative, and only then in conformance with the provisions of this Instruction.
5. Classified material shall not be taken further forward in combat areas than is necessary for efficient prosecution of the mission.

0902. DISSEMINATION OF CLASSIFIED INFORMATION

In the absence of specific exceptions authorized in accordance with the provisions of this Chapter, dissemination of classified information, shall be limited strictly to those persons whose official military or other governmental duties require such access in the interest of promoting national defense and who have been properly cleared for access thereto in accordance with standards equivalent to those in Chapter 15 of this Instruction. Responsibility for determining whether a person's official military or other governmental duties require that he possess or have access to any classified information and whether he is authorized to receive it rests upon each individual who has possession, knowledge, or comand control of the information involved, and not upon the prospective recipient. These principles are equally applicable whether the prospective recipient is an individual, a United States military command, a defense contractor, another Federal Agency, or a foreign government. Refer to sections 3, 4, 5, and 6 of this chapter for instructions regarding disclosure of classified defense information outside the Executive Branch of the Government or Department of Defense contractors.

0903. DISSEMINATION OF RESTRICTED DATA

The authorized dissemination for RESTRICTED DATA is as follows:
1. To persons in the Department of Defense whose official duties require information on the specific subject under consideration and to Department of Defense contractors and their employees when essential to the performance of a contract; provided in each such case, that all personnel concerned have been properly cleared to handle information of the highest classification category involved.
2. To persons other than in paragraph 1. above only on a "need to know" basis and only if they possess Atomic Energy Commission "Q" clearance.

0904. DISSEMINATION OF CLASSIFIED INFORMATION ORIGINATED OUTSIDE THE DEPARTMENT OF DEFENSE

Classified information which originates outside the Department of Defense shall not be disseminated

outside the Department of Defense without the consent of the originating agency.

0905. CONTROL OF TOP SECRET INFORMATION

1. All individuals having knowledge of Department of Defense information classified Top Secret shall be identifiable at all times; i.e., each organization or office originating or receiving information classified Top Secret shall maintain a list of those persons within such organization or office having access thereto. Access lists of recipients of Top Secret information will not be forwarded to the originating office except upon request.
2. Upon preparation or receipt of Top Secret information, each originator or recipient shall keep a record of the name of each individual, including stenographic and clerical personnel, who is afforded access to the Top Secret information originated or received.
3. Upon origination or receipt of Top Secret material in a Navy command or activity, a disclosure record form shall be attached immediately to the material and, thereafter, any individual gaining knowledge of the contents thereof shall affix to the form his name, the name of the activity, and the date of access. If an individual's signature is used and is not clearly legible, the name shall also be printed.
4. Disclosure record forms shall not be detached from the Top Secret material on which they are placed unless it is transmitted to another activity for retention. When such forms are detached, they shall be retained locally for a period of at least 1 year. After one year, they may be transferred to records centers for retention.
5. Mail rooms, file rooms, communication and message centers, and printing and reproduction activities engaged in processing large volumes of Top Secret material need not require assigned personnel to sign individually the disclosure record form if access to such areas is limited to permanently assigned personnel and if such individuals are identifiable by roster as having access on any given date.
6. Oral discussions within committees or at conferences involving the disclosure of Top Secret information are subject to the accountability requirements of this article. The minutes of the conference or meeting, showing a summary of the information discussed or furnished at the meeting, and a complete listing of all persons present at such meeting or conference, will be sufficient record for accountability requirements of this article. For detailed regulations governing disclosures through symposia and conferences refer to section 6 of this chapter.
7. Disclosure record forms do not supplant the requirement of article 0712 for executing a continuous receipt system for Top Secret material.

0906. CONTROL OF COPIES AND EXTRACTS

1. Material classified Top Secret and Secret originating outside the Department of Defense shall not be reproduced without the consent of the originating agency.
2. Originators of Top Secret documents shall insure, at the time of issuance, that all copies of each document are serially numbered and limited as to reproduction authority as required in articles 0607 and 0420.4.
3. Originators of classified material other than Top Secret, including RPS-distributed nonregistered publications, may limit the reproduction or extracting thereof as necessary. In no event, however, shall classified material be reproduced or excerpted without the approval of competent authority.
4. In reproducing classified documents on office-type copying equipment, care must be taken that the classification marking is not "lost". Such equipment does not always clearly reproduce all colors of ink or marginal images.

0907. DISSEMINATION TO INACTIVE PERSONNEL

Retired or reserve inactive personnel, regardless of rank, are not entitled to classified information merely by virtue of their present or former status. Unless they have been specifically authorized by the Chief of Naval Operations (Director of Naval Intelligence) to receive classified information, it shall not be disclosed to them. This does not limit the disclosure of classified information to inactive personnel who have been properly authorized access for purposes of training.

0908. DISSEMINATION TO RESERVE PERSONNEL FOR TRAINING

1. Reserve personnel on active duty for training may have access to classified information, including

RESTRICTED DATA, as necessary in the performance of their duties provided they have been properly cleared to handle classified information of the highest classification category involved.

2. Reserve personnel in an inactive status, if they have been properly cleared to handle classified information of the highest classification category involved, may have access to classified information at military commands or activities for training purposes under the following conditions:

a. Top Secret: Only with the approval of the Chief of Naval Operations (Director of Naval Intelligence). Disclosure will be authorized only if the training command certifies the release is necessary in the interests of national defense.

b. Secret: Only with the approval of the Commandant of the Marine Corps in the case of the Marine Corps Training Program; the Chief of Naval Air Reserve Training in the case of Naval Air Reserve drill units; and the Chief of Naval Personnel in case of all other Naval Reserve drill units (pay or non-pay). Disclosure will be authorized only when the classified information in question is needed in connection with planned training curriculum.

c. Confidential: As necessary to accomplish an assignment or to prepare for a mobilization billet.

3. Classified material, except that designated as Confidential — Modified Handling Authorized, shall not be released into the personal custody of inactive reserve personnel for removal from a military command or activity.

4. Inactive reserve personnel shall not be granted access to or be issued cryptographic aids, cryptographic publications, or RESTRICTED DATA.

Section 2

ORAL DISCUSSION AND PERSONAL CENSORSHIP

0909. PERSONAL CENSORSHIP

1. Indiscreet conversation and personal letters constitute great menaces to security. This applies especially to persons discussing office affairs with their families or friends. It also applies to careless talk on duty in the presence of persons not authorized to have the information. Loose talk in public places and over the telephone is also most dangerous. Information imparted to unauthorized persons within or outside the Naval Establishment may be repeated innocently and in ignorance of its importance until it becomes a matter of common knowledge. Foreign intelligence agents are scientifically trained to collect and to collate numerous bits of seemingly harmless information from conversation and rumors which circulate in the vicinity of naval activities. Therefore, automatic personal censorship of official and unofficial conversation and letters shall be a fundamental duty of all personnel of the Naval Establishment. The habit must be cultivated until it becomes routine.

2. When classified information is discussed orally, the audience shall be informed of its classification.

3. The debriefing of personnel leaving Department of Defense employment, or leaving the employment of Department of Defense contractors having classified contracts, must incorporate positive instructions against unlawful disclosures of classified information. Similar positive procedures shall be applied in the case of military personnel retiring or separating from the service. (Refer to article 0619.)

0910. TELEPHONE CONVERSATIONS

Classified information shall not be disclosed over telephones because of the insecurity due to executive cut-in, phantom voice interception, and wire tapping.

0911. APPROVED CIRCUITS

1. The Joint Chiefs of Staff have established a policy on approved circuits which governs the transmission in plain language of Secret and Confidential information over wire circuits. This policy is contained in the Joint Communication Instructions and establishes as a command responsibility the authorization for the transmission of classified information over wire systems.

2. No electrical circuit is approved for the transmission in plain language of any information having a classification of Top Secret.

0912. SECURITY OF UNUSUALLY SENSITIVE OPERATIONS

1. A commanding officer or officer in charge of a task force, a special operation, or other activity which in his opinion requires extraordinary security measures has authority to promulgate and enforce orders with respect to personal communications of military personnel. Such orders under the Uniform Code of Military Justice shall also apply to civilian personnel serving with, employed by, or accompanying the Armed Forces outside the continental limits of the United States and the following territories: That part of Alaska east of longitude one hundred and seventy-two degrees west, the Canal Zone, the main group of the Hawaiian Islands, Puerto Rico, and the Virgin Islands. Such orders may embody the substance of the following security measures to the extent considered essential by the command concerned:

a. Prohibition, or reduction to a minimum, for a designated period of time, of all outgoing personal telecommunications, except such emergency messages as may be specifically approved by the commanding officer of the operation; and

b. Prohibition, or reduction to a minimum for a designated period of time, of all outgoing personal correspondence; or

c. Inspection of outgoing personal correspondence prior to entering the U. S. mail system in the following manner:

(1) Personal communications intended for mailing to be deposited unsealed in designated receptacles;

(2) Such communications to be inspected for security violations by duty appointed representatives of the force commander, who will seal and deposit them in the U. S. mails, or, in case of security violations, will return them to the originator or hold them for appropriate corrective or disciplinary action as directed.

NOTE: Appropriate measures should be taken to insure that each inspector of each piece of mail can be subsequently identified. Such measures should minimize or exclude the possibility that the fact of inspection will become known to addressees. This may be accomplished by logging of outgoing mail or by assigning to each inspector a stamp bearing a number or sign to be inconspicuously placed on inspected mail. Wherever practicable, mail containing valuables should be inspected, sealed, and posted in the presence of the sender or of another witness. An inspector of mail should not inspect and release his own personal mail.

d. Prohibition of the use of private codes in any permitted communications.

e. Prohibition of mailing or otherwise despatching personal communications ashore in any manner to avoid such inspection controls as may be established.

f. Provision that all personnel concerned will initial such orders and by so doing indicate that they have read and understood them.

g. Provision for reminding all personnel concerned that Federal law prohibits unauthorized disclosures of classified information either during or after the particular operation and that appropriate disciplinary action will be taken against offenders.

2. The material in this article is presented as of possible assistance to commands and is not intended to limit commands in the application of whatever other cautions or security measures may be considered essential.

0913. PRISONERS OF WAR

1. The United States is a party to the Geneva Convention Relative to the Treatment of Prisoners of War (12 August 1949), and the provisions of this Convention are binding on personnel of the naval service.

2. Pursuant to the provisions of article 17 of the above Convention, each prisoner of war, when questioned on the subject, is bound to give only his full name, grade or rate, service number, and date of birth. All members of the naval service shall comply with these provisions in case of capture.

3. Prisoners can expect to be questioned upon capture. During such interrogations they shall not give any information other than their names, grades or rates, service numbers, and dates of birth. Threats, inducements, promises, and subterfuges might be used by the enemy to extract information. Seemingly harmless subjects, such as baseball and golf, should not be discussed while undergoing interrogation, as a trained interrogator can often extract the information he desires through such a

discussion. There is no such thing as a harmless subject of discussion while a prisoner is held in an enemy interrogation center. (See General Order No. 4, Code of Conduct for Members of the Armed Forces of the United States, 18 March 1957.) Prisoners shall endeavor to communicate promptly their names, grades or rates, service numbers, dates of birth, and prison addresses to the International Red Cross Committee, Geneva, Switzerland. No other information shall be given for use by the Red Cross.

0914. TESTIMONY BEFORE COMMITTEES OF CONGRESS AND EXECUTIVE COMMISSIONS, BOARDS, COMMITTEES, AND SIMILAR GROUPS

1. Classified naval information shall be made available to committees of the Congress and to executive commissions, boards, committees, or similar groups only when specifically authorized by the Secretary of the Navy (refer to SECNAV Instruction 5500.9 and SECNAV Instruction 5730.8 or subsequent revisions). The Secretary of the Navy will issue specific instructions as to the limits of disclosures as well as any other special instructions as to security which he deems appropriate.

   a. Chiefs of Bureaus and Offices of the Navy Department and the Commandant, U. S. Marine Corps are authorized to act for the Secretary of the Navy in permitting release of classified information to committees of the Congress when required in connection with the presentation of the budget and other legislation sponsored by the Secretary of the Navy.

2. Whenever a person in the Naval Establishment appears before a committee of the Congress, or an executive commission, board, committee, or a similar group, in either executive or public session, and is called upon to give testimony which includes classified information, he shall not divulge the information unless he has been authorized by the Secretary of the Navy or delegated authority to do so.

3. If a person in the Naval Establishment does not have authority to testify on classified matters, he shall respectfully state to the inquiring body that he is not authorized to disclose the information desired. He shall further inform the group that he will endeavor to obtain necessary authority, if the information desired by the body is specifically defined.

4. Personnel of the Naval Establishment, when called upon to testify as described in paragraphs 1 and 2 above, shall immediately endeavor to obtain necessary instructions from the Secretary of the Navy or delegated authority concerning the disclosure of information which they anticipate will be desired.

When a person in the Naval Establishment is requested to give testimony which includes classified information which he has been authorized by the Secretary of the Navy to disclose, he shall respectfully request that the testimony be given in executive session only. He shall further request that a record of such hearings not appear in the Congressional Record or any other document open to public inspection.

0915. LEGISLATION

1. Unless authorized by the Secretary of the Navy, information as to any legislative recommendation shall not be revealed to any individual or association not under Federal control, except as may be required by law. When release is made to other Federal activities, release shall be based on the "need to know" requirement.

2. Similarly, the nature and content of reports of the Department of Defense or of any military department or board within the Department of Defense, on bills referred by committees of Congress or by other Federal activities shall not be disclosed to any individual or association not under Federal control unless specifically directed by the Secretary of the Navy. When release is made to other Federal activities, such release shall be based on the "need to know' requirement.

Section 3

DISCLOSURE THROUGH JUDICIAL PROCEEDINGS

0916. GENERAL COURTS-MARTIAL

By law every person who has been tried by general court-martial is entitled to a copy of the record of the proceedings of the court, whether he was acquitted or convicted. Frequently, such copy is

delivered to civilian counsel for use as a basis for legal attack upon the conviction. Such records may be introduced into evidence in civilian courts, thereby becoming, in their entirety, public records. It is important, therefore, that every precaution be taken by convening authorities of general courts and by courts, law officers, and trial counsel to protect the security of classified information. It is, therefore, directed that officers who are authorized to convene general courts-martial shall make every effort to have all information to be introduced as evidence declassified.

1. If the trial of a case involves classified information, and the convening authority finds that the trial would be warranted except for the fact that it would probably be detrimental to the prosecution of a war or inimical to national security he shall, without dismissing the charges, forward the case to the officer exercising general court-martial jurisdiction over the command for disposition. If the latter officer concurs in the determination, he shall forward the case through channels to the Secretary of the Navy who may, in time of war, certify to the President that trial would be detrimental to the prosecution of the war or inimical to national defense. In such event, the applicable statute of limitations is extended to 6 months after termination of hostilities as proclaimed by the President or by joint resolution by Congress. Any officer exercising general court-martial jurisdiction has the authority to determine whether security considerations are paramount to trial, and he may, in appropriate cases, dismiss the charges or authorize their trial instead of forwarding them to the Secretary.

2. If classified information is required for prosecution and the trial is authorized, the officer exercising general court-martial jurisdiction shall be governed by the following procedures:

a. Grant appropriate personnel security clearances in accordance with chapter 15 of this manual to all members of the court, members of the prosecution and defense, and the court reporters.

b. If the accused is represented by civilian defense counsel, such counsel must likewise have been cleared before classified information may be disclosed to him. In no case shall a clearance of a civilian defense counsel be based on investigation action less than a National Agency Check.

c. Sessions of the court-martial shall be closed to the public whenever necessary to prevent dissemination of classified information to other than authorized persons.

d. The original record of trial shall be properly classified.

e. If the copy of the record prepared for the accused contains information requiring security protection, the trial counsel, unless otherwise directed by the convening authority, shall forward the accused's copy to the convening authority. The latter shall excise or withdraw from the accused's copy any information requiring security protection and will, thereafter, cause expurgated copy to be delivered to the accused together with a certificate to the effect that certain information has been deleted or withdrawn from the accused's copy of the record for reasons of national defense and that the original record of trial may be inspected in the files of the Judge Advocate General of the Navy under such regulations as may be prescribed by the Secretary of the Navy.

f. The certificate shall list:

(1) The pages from which information has been deleted.

(2) The pages which have been removed in their entirety.

(3) The exhibits which have been withdrawn.

A copy of this certificate, together with a statement signed by the accused acknowledging receipt of an expurgated copy of the record of trial, or a certificate of delivery of same, shall be attached to the original record of trial.

g. If the necessity for assigning classification is determined subsequent to delivery of a copy to the accused, the copy shall be recovered by proper authority and returned to the convening authority for expurgation.

0917. PRODUCTION OF OFFICIAL RECORDS IN CIVIL COURTS

1. Classified information shall not be released for introduction into civil courts.

2. In cases where naval records are desired by or on behalf of litigants and where the records are not classified or of a privileged status as described in article 1251, Navy Regulations, such parties

shall be informed that the procedure for the production of the records desired or of certified copies thereof is to obtain and forward to the Secretary of the Navy, Department of the Navy, Washington, D. C., a court order calling for the particular records desired or copies thereof. Compliance with such court orders, after authorization by the Secretary of the Navy or his designee, shall be effected by transmitting certified copies of the records to the clerk of the court from which the process was issued or by production of the original records, where necessary. Where an original record is produced it shall not be removed from the custody of the person producing it but copies may be placed in evidence in the case. Upon the written request of all parties in interest or of their counsel, records which would be produced in response to a court order as above set forth may be furnished without such court order; provided, however, that the production in Federal, State, or Territorial courts of the service, employment, pay, or medical records of personnel of the Navy, Marine Corps, and Coast Guard including civilian employees thereof, is authorized upon receipt of a court order where litigation is pending without procuring specific authority from the Secretary of the Navy.

3. Where official records are desired for use in a matter not in litigation, and where the records are not classified or of a privileged status as described in article 1251, Navy Regulations, a written request for said records by the parties in interest or their counsel shall be sent to the Secretary of the Navy (Judge Advocate General), Department of the Navy, Washington, D. C. When the purpose for which the records are desired is in the judgment of the Secretary of the Navy (Judge Advocate General) sufficient to justify compliance with the request and the interests of the Government would not be predjudiced thereby, the Secretary of the Navy (Judge Advocate General) may release such of the official records as he may determine to be appropriate under the circumstances.

0918. CLAIMS AGAINST THE UNITED STATES

No person in the Naval Establishment other than in the discharge of his official duties shall disclose any information whatever, whether classified or unclassified, or whether obtained from official records or within the immediate knowledge of the relator, which might be of aid or assistance in the prosecution or support of any claim against the United States (18 U. S. C. 283).

0919. COLLISION CASES

In those cases wherein a naval ship was involved in collision, an opportunity for survey of the naval ship shall not be permitted if such survey will invoke possible disclosure of classified information. In such cases, the representatives of the other ship, craft, or structure shall be advised that in the interests of national defense an opportunity for survey of the naval ship will not be afforded.

Section 4

DISCLOSURE TO FOREIGN GOVERNMENTS

0920. GENERAL POLICY

1. No person in the Naval Establishment shall convey orally, visually, or by written communication any classified information to any foreign national or foreign government unless such disclosure has been specifically authorized in writing by the Chief of Naval Operations (Director of Naval Intelligence). In exceptional cases, where the required approval is furnished by telephone or other oral means, prompt confirmation in writing must be obtained.

2. United States citizens who serve as representatives, officials, or employees of a foreign government, firm, corporation, or individual shall be considered as foreign nationals when acting in such capacity.

3. Unclassified information may be disclosed to foreign nationals or foreign governments, provided any such disclosure is in accord with article 1252, Navy Regulations.

0921. TRAINING FOREIGN NATIONALS

Each request for admission of a foreign national to a classified course of instruction or training shall be referred to the Chief of Naval Operations (Director of Naval Intelligence). Each admission

of a foreign national to such instruction or training shall be decided on its merits, after the advice of the interested bureaus and offices concerned has been obtained. No precedent will be considered as established by the granting of a specific request.

0922. INTERNATIONAL TRAFFIC IN ARMS

The State Department administers the international traffic in arms and military material in accordance with the policies set forth in "Regulations Governing the International Traffic in Arms, Ammunition, and Implements of War and Other Munitions of War." In this connection, the State Department does not release for foreign sale any item of classified military equipment until the Departments of the Army, Navy, and Air Force have stated that there is no objection to the release. The Chief of Naval Operations shall render decisions for the Department of the Navy in this regard.

Section 5

DISCLOSURE OUTSIDE THE EXECUTIVE BRANCH

0923. GENERAL POLICY

No person in the Naval Establishment shall convey orally, visually, or by written communication any classified information outside the Executive Branch of the Government of the United States unless such disclosure has been specifically authorized by the Chief of Naval Operations (Director of Naval Intelligence) except as provided in article 0924 below.

0924. DISCLOSURES TO DEPARTMENT OF DEFENSE CONTRACTORS

Bureaus and offices of the Navy Department may make disclosures of Navy classified information to private activities in connection with production, procurement, research and development, and maintenance contracts or programs of the Department of Defense without prior approval of the Chief of Naval Operations (Director of Naval Intelligence), subject to the provisions of paragraphs 1 through 4 below. Insofar as disclosures to private activities are concerned, it is required that there be a bona fide contractual relationship existing between a private organization (or members thereof) and an element of the Department of Defense; except that this is not intended to prevent essential disclosures involved in pre-contract negotiations with an appropriately cleared facility. These provisions likewise apply to sub-contracts and contracts with consultants (Personal Services Contracts).

1. Disclosure of classified information to private contractors shall be made in accordance with paragraph 2–115 of the Armed Forces Industrial Security Regulation (OPNAV Instruction 5540.8A or subsequent revisions.) Classified information may be divulged to a contractor only on a "need to know" basis, provided the contractor has an active facility security clearance of the appropriate category. Prior to granting physical custody of Department of the Navy classified material to Department of Defense contractors, the forwarding activity must determine that the contractor has the ability to physically safeguard the classified material. (When the forwarding activity does not have information as to the clearance and/or safeguarding status of the contractor, a determination should be made from the Military Department activity having security cognizance of the facility.)

2. Release of information shall not prejudice the interest of the source and shall not violate any commitment made in obtaining the information under consideration.

3. Industrial or commercial proprietary information, including information relating to trade secrets, processes, operations, materials, style of work or apparatus, statistics relating to costs or income, profits or losses shall not be published or disclosed by a bureau, office, activity, official, or employee of the Department of the Navy receiving such information, without the express written permission of and in strict accordance with any conditions stated by the legal proprietor of such information.

4. Restrictions on the release of the information imposed previously by a competent authority shall govern in each such case.

0925. OTHER DISCLOSURES

1. The Chief of Naval Operations (Director of Naval Intelligence) may authorize other disclosures outside the Executive Branch of the Government of the United States if in the interest of promoting national defense. Requests for such disclosures shall be in writing. Requests shall state the reason the classified information is desired and the intended use thereof.

2. All disclosures are subject to the following:

a. That the recipient is informed of the classification of the information divulged.

b. That the recipient is informed of handling and stowage requirements.

c. That the recipient is informed of his liability in the event of unauthorized disclosure. (Refer to article 0432 and 0433.)

d. When Top Secret information is authorized to be released outside the Department of Defense, such authorization shall include the following statement:

> "This information is released under the condition that a record be kept by the recipient of all individuals who are afforded access to the information contained in the document, and that this record will be made available to the Department of Defense if requested."

In addition, the office of issuance of the Top Secret document will be informed of the outside dissemination.

e. All classified material shall be covered by receipts.

Section 6

DISCLOSURE THROUGH CONFERENCES AND SYMPOSIA

0926. GENERAL POLICY

A bureau or office of the Navy Department may, under the authority granted in article 0924 of this manual, disclose classified information to conferences, symposia, and gatherings which it sponsors and which are composed of persons under contract to the Department of Defense. Release under this authority must be on a basis that the information is needed in the specific performance of contracts or services (in the case of consultants) involved and is conditional upon the participants having appropriate security clearances.

0927. APPROVAL REQUIRED BY THE CHIEF OF NAVAL OPERATIONS (DIRECTOR OF NAVAL INTELLIGENCE)

1. Except as authorized in article 0926 above, all disclosures of Navy classified information at conferences, symposia, or gatherings including persons outside the Executive Branch of the Government of the United States require the approval of the Chief of Naval Operations (Director of Naval Intelligence). Requests for release of classified information will be refused unless there is a clear determination by appropriate naval authority that the national defense interest will specifically gain thereby, and that alternative, conventional channels of release will not be productive.

0928. NAVY SPONSORSHIP

1. All meetings of scientific and technical associations must be sponsored by a Navy command or activity before disclosure of Navy classified information will be authorized. Sponsorship includes responsibility for assuring that adequate measures will be taken to protect the classified information to be disclosed and that all prospective recipients have a legitimate "need to know", as well as assuring that they are good security risks and have active security clearances for the highest classification category involved.

2. It is not the intent of paragraph 1 above that a Department of the Navy command or activity co-sponsor meetings already sponsored by another department or office of the Executive Branch of the Government at which personnel of the Naval Establishment are invited to disclose Department of the Navy classified information. In such cases, however, members of the Naval Establishment shall not disclose classified information until officially authorized by their command or activity. Prior to authorizing or seeking approval for such disclosures the responsible command or activity should assure itself through official channels that a reported official sponsorship by another department or office of the Executive Branch is genuine,

and that the term "sponsorship" is given the same significance as that set forth in paragraph 1 above.

0929. INFORMATION REQUIRED TO PROCESS REQUESTS

In order for the Chief of Naval Operations (Director of Naval Intelligence) to make a determination in each case as required by article 0927, the following information shall be furnished by the interested Naval activity:

1. A clear statement as to the necessity for the disclosure.
2. The category of the classified information to be disclosed and a brief summary of its content.
3. Nationality and name of any foreign government representative who will attend the conference.
4. And in addition, when the conference is under Navy sponsorship, the following personal data are required for proposed participants who are not properly cleared members of the Executive Branch of the Government or cleared Government contractor personnel:
   a. Full name, date and place of birth.
   b. Occupation and organization they will represent at the proposed conference.
   c. Present home and business addresses.

0930. TIME REQUIRED

Requests must be received by the Chief of Naval Operations (Director of Naval Intelligence) at least 1 month prior to the date of the proposed meeting in order to provide adequate time for processing.

0931. PHYSICAL SECURITY PROTECTION

The sponsoring activity must arrange for suitable quarters for the classified conferences and make certain that adequate security measures are maintained throughout the period of the meeting. Such measures include but are not limited to the following:

1. Arrangement for admission of only those persons authorized to attend. All individuals must produce positive identification.

2. Cautionary statements to those attending the conference as to any special security practices to be observed.

3. Arrangements for adequate stowage or protection of classified material handled during the meeting, and provisions for insuring return of all classified material furnished to those present.

4. Take all practicable precautions to minimize any danger of inadvertent disclosure of classified information through the use of listening or recording devices. (See article 0616.4).

Chapter 10
DISCLOSURE THROUGH PUBLIC RELATIONS

1001. RESPONSIBILITY

1. The Secretary of the Navy is responsible for informing the citizens of the United States concerning the naval activities of their Government. He normally accomplishes this through the Chief of Information. Basic guidance may be found in SECNAV Instruction 5720.7 (U. S. Navy Public Information Manual) or subsequent revisions.

2. The Chief of Naval Operations (Director of Naval Intelligence) shall inform the Secretary of the Navy (Chief of Information) with regard to current military security policy as related to public dissemination.

3. Upon request, or as otherwise may come to his attention, the Director of Naval Intelligence shall inform the Chief of Information as to the classification of specific information under consideration for release to the public. In many cases specific guidance concerning releases of information of this type already exists: SECNAV Instruction 5511.23, which deals with the release to the public of information on guided missiles, military aircraft, associated powerplants, components and/or accessories; SECNAV Instruction 5511.24, on the same subject; and SECNAV Instruction 5511.11, which sets forth the authority for declassifying information relating to new developments, new equipment, or new operational techniques.

4. The Director of Naval Intelligence and the Chief of Information shall maintain the closest possible liaison in order that the obligation to disseminate information of proper and legitimate public interest can be accomplished without compromising security.

1002. RELEASE TO PUBLIC

1. In the interests of national defense, classified naval information shall not be released to the public.

2. Normally, information which is to be released to the public shall be disseminated through duly established public information officers.

3. So-called off the record interviews are not authorized.

1003. CHARACTER OF RELEASES

1. The American public is entitled to know as much about its Navy as security limitations permit. To this end, releases should include unclassified information on any aspect of the Navy or its activities in which the public has a legitimate interest. Releases may include information which is broad in scope and which show a relationship to national policy, or they may include unclassified technical or scientific information designed to stimulate research and aid American science and industry.

2. The work of foreign intelligence agents is greatly simplified by the easy collection of technical facts which appear in publications available to the general public. From an intelligence standpoint, the time and effort which foreign agents must expend to collect such information if it is not made available to the public are very costly and subject the personnel involved to being apprehended for violation of Federal laws. By compelling foreign agents to expend time and money in the collection of such information, their efforts on other projects are automatically curtailed.

3. No unclassified information relating to performance or capabilities of new weapons or new equipment of any type, or to modifications or improvements to existing weapons or equipment which result in improvement of military performance, shall be released to the public without specific reference to the Secretary of the Navy for clearance by the Secretary of Defense.

1004. INFORMATION OF JOINT INTEREST

Information of joint Army-Navy-Air Force interest shall not be released unless its disclosure is authorized by the Office of the Secretary of Defense after clearance with each of the military services.

1005. EFFECT OF RELEASES

The authorized or unauthorized release for publication by the press, radio, or other media of specific information on a subject does not in itself declassify all related information on the same subject. Unauthorized publication is not acceptable as a reason for declassification or authorization for further publication. Known compromise of classified information does not of itself constitute a declassification or even a downgrading of that information. Regrading of compromised information remains subject to official action by competent authority.

1006. RELEASE OF RESTRICTED DATA

RESTRICTED DATA as defined in the Atomic Energy Act of 1954 shall not be released to the public.

1007. RELEASE OF CRYPTANALYTIC DATA

1. No information shall be released to the public or to unauthorized private individuals concerning cryptanalytic processes except as specifically approved by the President in each case.
2. Information with regard to cryptanalysis shall be controlled as follows:
   a. The past or present status of cryptanalysis systems, techniques, and procedures shall not be divulged in any manner.
   b. The degree of success attained or specific results achieved, either past or present, by any cryptanalytic unit operating under governmental authority shall not be divulged in any manner by any organization or individual. (Refer to Act of 31 October 1951, appendix F.)

1008. COMMERCIAL RELEASES AND ADVERTISING

1. Release of information by Navy contractors is covered by the provisions of OPNAV Instruction 5540.8A (Armed Forces Industrial Security Regulation); the Industrial Security Manual for Safeguarding Classified Defense Information; SECNAV Instruction 5720.3; and such other directives as from time to time may be issued.
2. Commercial firms may advertise that their products are in use by the Naval Establishment. Such advertising may be granted naval clearance if the following provisions are met:
   a. No classified information is divulged.
   b. The advertising constitutes a statement of fact with no misleading or otherwise objectionable features.
   c. No mention is made to indicate that a product has undergone service tests. Data from service tests shall not be disclosed.
   d. No statement is made that the product is used by the Naval Establishment to, the exclusion of, or in perference to, other similar products.
   e. Contents do not reflect discredit on the Naval Establishment or other governmental establishments.
   f. All copy, texts, and photographs connected therewith are submitted for Navy review prior to release or clearance. In cooperating with an advertiser, the Navy shall not assume responsibility for accuracy of the advertiser's claims or for his compliance with laws protecting the rights of privacy of military personnel whose photographs, names, or statements appear in the advertisements.

1009. PUBLIC SPEECHES AND PUBLICATION OF ARTICLES OR BOOKS

1. The inclusion of classified information in any article, book, speech, or public discussion by a naval member or civilian employee of the Naval Establishment for dissemination outside the Naval Establishment is prohibited.
2. Public speeches or published articles or books are not to be presented as "official" or reflecting the views of the Department of the Navy without the written approval of the Secretary of the Navy. (Refer to Article 1252, U. S. Navy Regulations, and OPNAV INST 5700.2)

1010. SHIP AND STATION NEWSPAPERS

Commanding officers shall be responsible for determining that classified information is not disclosed by informal ship and station publications and newspapers which are published under their jurisdiction for general issue.

Chapter 11
CONTROL OF PHOTOGRAPHY

1101. RESPONSIBILITY

1. Persons in a command status shall be responsible for controlling the photographing of all material within their jurisdiction. This applies to official and unofficial photography, regardless of whether the photographers are attached to the Naval Establishment or are private citizens. Additional directives shall be promulgated by commands as necessary to control photography within the respective command.
2. When competent authority higher than the commanding officer authorizes the taking of official or unofficial photographs, such authority in no way relieves the local authority from responsibility for supervision, censorship, and release of resulting photographs, unless so specified.
3. The taking of unofficial photographs within naval jurisdiction is forbidden, unless specifically authorized.
4. Visitors shall not be allowed to take photographic equipment into a naval shore establishment or on board a naval ship or aircraft unless specifically authorized by the commanding officer.

1102. PHOTOGRAPHS BY NAVAL PERSONNEL AND DEFENSE CONTRACTORS

1. A commanding officer, or higher authority, may authorize naval personnel or defense contractors to act as official photographers for his command. Developing and printing incident thereto shall be accomplished under naval jurisdiction.
2. Naval personnel shall be allowed to bring cameras on board ships and aircraft or into shore installations only as authorized by commanding officers and subject to such restrictions for the protection of classified information as they may impose. They shall not be used on board ship for official or unofficial purposes without the authorization of the commanding officer. In case the commanding officer authorizes the use of cameras on board for unofficial purposes, he shall insure that resulting photographs do not reveal classified information.

1103. PHOTOGRAPHS BY COMMERCIAL PHOTOGRAPHERS

1. All photographs taken on board a naval ship or aircraft or in any shore establishment by commercial photographers representing public news media shall be submitted to the commanding officer, or other designated officer, for review. If such photographs are determined to be classified, they shall be assigned an appropriate classification and forwarded, with all negatives and copies thereof, to the Secretary of the Navy (Chief of Information).
2. All commercial negatives and prints shall remain under naval jurisdiction until officially released.

1104. ADVISER TO PHOTOGRAPHERS

In the mutual interest of the Navy and organizations engaged in photographic work, whenever a civilian photographer ("still" or "motion picture") is authorized to take naval pictures, a qualified officer shall act in an advisory capacity to the photographer so as to prevent unauthorized disclosure.

1105. TRAINING FILMS

Contracts for commercial production of Navy training films shall include adequate and detailed safeguards to prevent the compromise of any classified information. (Refer to The Armed Forces Industrial Security Regulation.)

1106. AERIAL PHOTOGRAPHS AND MAPS

The policy on classification and release of aerial photographs is contained in OPNAV Instruction 5511.19 or subsequent revisions.

1107. TELEVISION

The general guidance contained in the preceding articles of this Chapter applies equally to television. However, the impossibility of conducting a security review during live television broadcasts makes it imperative that commanding officers take all necessary measures to prevent deliberate or inadvertent disclosure of classified information on those occasions. In most cases this will require a careful survey well before broadcast time not only of the immediate objects being featured but also of the entire background.

1108. MARINE CORPS PROVISIONS

The Commandant, United States Marine Corps, shall exercise primary control of photographs which relate to the activities of the Marine Corps. In exercising such authority, he shall conform to this publication and other basic directives.

1109. MISCELLANEOUS

The directives contained herein shall be applicable to artists, sketchers, and draftsmen in the same manner as to photographers.

Chapter 12
REPRODUCTION OF CLASSIFIED INFORMATION

1201. RESPONSIBILITY

1. The Secretary of the Navy (Administrative Officer, Navy Department) has technical control over the planning, preparation, printing, reproduction, and distribution of all Navy classified publications (except registered publications) regardless of where initiated or accomplished. The Secretary of the Navy (Administrative Officer, Navy Department) will issue such additional instructions as are necessary to fulfill his responsibility.
2. Local commands are responsible for the planning, preparation, printing, reproduction, and distribution of classified information developed or produced within the limits of their respective commands, subject to the instructions promulgated by the Secretary of the Navy (Administrative Officer, Navy Department).

1202. SCOPE

1. These security measures apply to all graphic arts functions including (1) the preparation or development of manuscript, art-work, layouts, or other original copy; (2) the production or reproduction of classified information by any basic, adapted, or substitute process of printing or reproduction and related methods; (3) film processing, binding, distribution and mailing, and all other processes involved in graphic arts.
2. The requirements of this chapter supplement the other chapters of this manual and must be read and construed in the light of other pertinent security regulations contained herein.

1203. INDUSTRIAL PRINTING SECURITY

The Secretary of the Navy (Administrative Officer, Navy Department) will provide technical assistance to the Office of Naval Material for carrying out the security measures for the protection of classified information in the graphic arts industry, and shall determine the requirements for the use of commercial graphic arts facilities in the preparation, production, reproduction, and distribution of Navy classified publications.

1204. PREPARATION, PRINTING, AND REPRODUCTION OF CLASSIFIED INFORMATION

Classified information shall normally be prepared, printed and reproduced by Navy or Department of Defense facilities. Where this is not possible, preparation, printing and reproduction of classified information is authorized only by the following:

1. For Top Secret:
   a. As specifically approved by the Secretary of the Navy (Administrative Office, Navy Department).
2. For Secret and Confidential:
   a. Government Printing Office.
   b. In commercial facilities having an active facility clearance at least as high as the classified information to be processed and obtained in accordance with the requirements of the Armed Forces Industrial Security Regulation and when specifically approved by the Secretary of the Navy (Administrative Office, Navy Department).

1205. SALE OF CLASSIFIED DOCUMENTS

The Printing Act contained in title 44 of the U. S. Code provides that a certain number of copies of each publication printed by order of an executive department may, under certain conditions, be sold or distributed to Government agencies or the general public. This act also provides that information which is of a "confidential character" and of no public interest shall not be sold to the general public nor otherwise be given public distribution. Classified naval publications shall not be sold to the general public or otherwise distributed outside of the Executive Branch except under the provisions of article 0923.

Chapter 13
COMMUNICATION SECURITY

1301. RESPONSIBILITY

1. Persons in a command status are responsible for the maintenance of communication security within their commands, and for impressing on all personnel concerned the vital importance to the United States of maintaining crypto-security. They shall also be responsible for the promulgation of additional directives, as necessary, to ensure proper communication security control within their jurisdiction.

2. As a basic responsibility, it is mandatory that all communication personnel comply with all security directives for classified information in general as well as with those which apply to communication security in particular.

3. The communication officer of a command is responsible to his commanding officer for compliance with the communication directives in connection with the encryption and transmission of messages.

4. The originator of a message is responsible for determining the necessity for transmission as a message rather than as a letter. He is also responsible for assigning classification and precedence.

1302. COMMUNICATION SECURITY INSTRUCTIONS

1. Detailed regulations and instructions regarding communication security are contained in joint, combined, and Navy communication instructions, the Registered Publication Manual, and operating instructions for the various crypto-systems.

2. Other details of communication security are presented in this manual as follows:

a. Telephone conversations — article 0910.

b. Information for public release based on encrypted messages — article 1304.

c. Release of cryptanalytic data — article 1007.

1303. CRYPTO-SYSTEMS

1. Crypto-systems shall be used only by authorized persons who are thoroughly familiar with regulations and instructions pertaining thereto.

2. The commanding officer shall insure that all members of cryptoboards are thoroughly familiar with the operating instructions for crypto-aids and currently effective communication security rules.

3. Personnel engaged in duties involving cryptographic material will be cleared strictly in accordance with specific instructions issued by the Chief of Naval Operations (Director of Naval Communications).

1304. HANDLING OF CATEGORY A, AC AND B MESSAGES

1. The edited plain text of a message marked "Paraphrase not required" (Category A or AC message) is subject to handling as follows without the necessity for paraphrasing:

a. It may be handled as correspondence of the same classification, including the mailing of copies, provided such handling is within the Department of Defense.

b. If distribution outside the Department of Defense in classified form is desired, the cryptocenter should be consulted for mandatory security precautions which must be taken prior to such distribution. In the event that consultation with the cryptocenter is impracticable, distribution in classified form outside the Department of Defense (including distribution to foreign nations) may be effected after the following security precautions are taken: the routing indicators, call signs, address groups, and internal references by date-time group shall be physically removed. The date-time group and/or internal reference number of the message may be retained for identification purposes.

c. If otherwise permissible, it may be declassified as a whole, provided the security precautions listed in subparagraph 1304.1.b. above are taken. Additionally, if the message is Category AC, the date-time group and the internal reference number, if there is one, shall be physically removed. Only the date of a Category AC message may be retained for identification purposes. The date-time group and/or internal reference number of a Category A message may be retained for identification purposes.

2. The edited plain text of a message marked "Paraphrase required" (Category B message) must be serially numbered and accounted for, and is subject to handling as follows:

a. When handled within the Department of Defense, paraphrasing is not required unless copies are mailed. If the transmission of a Category B message is accomplished by officially designated courier, paraphrasing is not required.

b. If either distribution outside the Department of Defense in classified form or declassification is desired, the cryptocenter should be consulted for mandatory security precautions which must be taken prior to such distribution. In the event that consultation with the cryptocenter is impracticable, distribution or declassification may be effected after carefully paraphrasing the original text and applying the following maximum security precautions: the date-time group, internal reference number if there is one, routing indicators, call signs, address groups, all internal references by date-time group, and Category markings shall be physically removed. Only the date of the message may be retained for identification purposes.

3. When it is desired to declassify messages dated prior to 1 February 1946, see OPNAV Instruction 02210.7 series, which permits exceptions to the declassification procedures outlined above.

4. Additional plain-text copies of Category B messsages shall be made only by the cryptocenter. All copies shall be serially numbered and receipted for.

5. When authorized, edited plain text copies of Category B messages, paraphrased or unparaphrased, shall be destroyed by burning by the custodian thereof in the presence of a witnessing officer. The destruction shall be recorded, and the record shall show the date and place of destruction, identity of the message, copy number, and the signatures of the custodian and the witness.

6. The encrypted and clear text versions of messages shall not be transmitted by U. S. mail under the same cover. If, under unusual circumstances, it should become necessary to transmit them together, they shall be transmitted by officially designated courier.

Chapter 14
VISITOR CONTROL

Section 1
GENERAL

1401. RESPONSIBILITY

1. The Chief of Naval Operations is responsible for the formulation and promulgation of the policy governing visits to activities of the Naval Establishment.

2. Persons in a command status shall be responsible for the security control of visitors within the limits of their jurisdiction. They shall promulgate such additional directives as are necessary for the control of visitors within their respective commands.

1402. VISITORS

The term "visitors" as used herein for security purposes applies as follows:

1. A visitor on board a ship or aircraft is any person who is not a member of the ship's company or not a member of a staff using the ship as a flagship.

2. A visitor to a naval shore esablishment is any person who is not attached to or employed by the command or staff using that station as headquarters.

1403. CATEGORIES OF VISITORS

Persons who are considered visitors as described in article 1402 are divided into three basic categories which are further subdivided as follows:

Category One — *United States citizens and immigrant aliens, except those representing a foreign government or a foreign private interest.*

- Alfa — Personnel of the Executive Branch of the Government involved in day to day working relations with members of the activity of the Naval Establishment to be visited and personally known to them.
- Bravo — Other Department of Defense and United States Coast Guard personnel.
- Charlie — Personnel of private facilities under contract to the Department of Defense.
- Delta — Other employees of the Executive Branch of the Government.

Category Two — *United States citizens and immigrant aliens not described in Category One.*

- Alfa — Representatives of a foreign government or military service.
- Bravo — Representatives of a foreign private interest.
- Charlie — Other United States citizens and immigrant aliens.

Category Three — *Foreign nationals (including foreigners in the United States on nonimmigration visas).*

- Alfa — Representatives of a foreign government or military service.
- Bravo — Representatives of a foreign private interest.
- Charlie — Foreign nationals in the United States sponsored by a military department, or other foreign nationals employed on military projects, either as contractor's employees or departmental employees.
- Delta — Other foreign nationals.

1404. RESPONSIBILITIES OF THE COMMAND BEING VISITED

1. The commanding officer of the activity being visited has full discretion as to whether or not the

visit shall be permitted. The granting of authorization for a visit, even though emanating from higher authority than the command being visited, shall be interpreted as an indication that competent authority has no objection to the visit at the time and under the conditions specified. Unless specifically requested or directed by competent higher authority, changes should not be made in the normal routine or operating schedule if they significantly interfere with the accomplishment of the primary mission of the command.

2. The term "subject to any restrictions deemed necessary", when used in connection with the authorization of visits, shall be interpreted as permitting the commanding officer of the activity being visited to impose any restrictions necessary to exercise his responsibility of safeguarding the classified information under his jurisdiction.

3. In keeping with the policy set forth in article 1514, commanding officers shall recognize clearances for access to classified information granted to visitors by competent authority. As is set forth in paragraphs 1 and 2 above, however, the commanding officer is not relieved thereby of the responsibility of determining the visitor's "need to know" or from his duty to withhold classified information when he considers such action necessary.

1405. VISITORS' RECORDS

Commanding officers shall maintain a record of all visits by persons in Categories Two Alfa and Bravo, and Three except during general visiting. This record shall consist of the name and signature, and if practicable the nationality, title, office and sponsor of the visitor, clearing authority if the visit involves access to classified information, the date and duration of the visit, and the name of the escort when utilized. These records shall be retained for 2 years.

1406. VISIT REPORTS

When any visitor expresses an undue interest in information that he is not authorized to receive, or expresses feelings inimical to the best interests of the United States, commanding officers and other naval representatives shall transmit immediately a complete report of the circumstances to the Chief of Naval Operations via the chain of command. An advance copy shall be forwarded directly to the Chief of Naval Operations. Reports shall include the following:

1. Name, title, or position (provide first, middle, and last names).
2. Nationality.
3. Sponsor.
4. Authority for visit.
5. Items of particular interest to the visitor.
6. General type of questions asked.
7. Expressed object of the visit.
8. Estimate of the real object of the visit.
9. General estimate of ability, intelligence, and technical knowledge of the visitor and his proficiency in the English language.
10. Exactly what was shown, explained, and refused.

1407. VISITOR CONTROL AND ESCORT

In order to protect the classified information under his jurisdiction the commanding officer shall cause the movements of all visitors to be restricted as he may deem necessary. When escorts are utilized, they are responsible to the commanding officer to ensure that the visitor has access only to that information which he has been authorized to receive. Escorts may be either military or civilian members of the Naval Establishment.

Section 2
UNCLASSIFIED VISITS

1408. GENERAL

1. Visits to activities of the Naval Establishment by persons who will not have access to classified information do not require authorization from the Chief of Naval Operations (Director of Naval Intelligence). The commandiing officer concerned is responsible for the conditions under which such visits are permitted, provided, however, that all

visitors in categories Two Alfa and Bravo, and Three shall be accompanied by a competent escort (refer to article 1407), except during general visiting (see article 1409).

1409. GENERAL VISITING

1. The Chief of Naval Operations will announce the periods for general visiting on special occasions of national significance such as Armed Forces Day. Prior approval for general visiting at any other time shall be requested as follows: fleet units visiting U. S. ports, from Senior Officer Present Afloat; fleet units visiting foreign ports, from Commander ordering the visit; shore stations and district vessels in the United States, from district commandants; and overseas shore stations, from the naval area commander. General visiting should be allowed only when the best interests of the Nation and the Navy will be served thereby. All general visiting shall be on an unclassified basis: i.e., no classified areas or information shall be shown or divulged to the general public.

2. Visits by special groups of individuals or visits designed to achieve a special purpose may be permitted on an unclassified basis, subject to prior approval as outlined above for general visiting, or subject to such standing instructions as those authorities may promulgate.

3. Commanding officers shall prepare a general visiting bill. This bill shall show the areas which may be open for general visiting. It shall describe the safeguards which shall be observed. During general visiting access should not be permitted to spaces containing classified or sensitive equipment unless such equipment has been concealed and adequately protected. Examples are plotting rooms, coding rooms, combat information centers, radio rooms, sonar spaces, and fire control or radar spaces. Care should be taken to avoid inadvertent disclosure of classified operational characteristics of ships or aircraft, either through conversation or by permitting access to instruments from which such data may be inferred.

4. As differentiation between people during general visiting is impracticable, the standard visiting bill shall be based on the probable presence of foreign agents among the visitors.

5. Bona fide friends and relatives of naval personnel, or other persons on legitimate business, may visit ships and naval shore activities subject to local regulations and provided no classified information is disclosed to the visitors.

6. Crews shall be instructed not to discuss the design and operational features of classified equipment with visitors.

1410. VISITS TO SHIPS BY FOREIGN PERSONNEL (see also article 1419)

1. The increasing cooperation between the Armed Services of the United States and those of numerous other nations has resulted in more frequent contacts between U. S. and foreign units and personnel. As a result, commanding officers are often faced with requests from varied sources to authorize visits of foreign personnel. (OPNAV Instruction 3128.3B contains instructions concerning visits by U. S. Naval vessels to foreign countries.)

2. In foreign countries in which United States military representatives are serving, requests for visits of foreign military personnel to United States naval ships not involving disclosure of classified information are normally made by the senior United States naval or other military representative direct to the commanding officer. The commanding officer of a ship is authorized to approve such visits at his discretion and subject to local restrictions established by higher authority.

3. Any United States commander, when he feels it to be in the best interests of the United States, may invite or permit important foreign nationals to visit aboard ship. Such visits should be conducted on an unclassified basis. On those occasions when access to classified information is considered necessary, permission will be obtained in accordance with provisions set forth in article 1419.

1411. VISITS TO NEW CONSTRUCTION OR SHIP CONVERSION PROJECTS

Visitors shall not be allowed on board ships under construction or conversion except on the authority of the Chief, Bureau of Ships, or his authorized field representative at the site of construction or conversion.

1412. DEPARTMENT OF THE NAVY SPONSORSHIP OF UNCLASSIFIED VISITS TO FOREIGN COUNTRIES

The sponsoring activity shall take all practicable measures to establish the propriety of sponsoring an individual prior to nominating him to visit a foreign country. (The individual's professional stature and capability and his local reputation will be taken into account. If considered desirable or necessary file checks may be made with the District Intelligence Officer or with the Office of Naval Intelligence as appropriate.)

1. Visit notifications: Sponsoring activities whenever possible shall notify the cognizant naval attache direct at least thirty (30) days in advance of the proposed visit and shall provide the following information:

a. Name of visitor (and activity or organization with which associated if other than the originator of the letter or message).
b. Title or rank of visitor.
c. Identification number when available (passport or I. D. card number).
d. Activities to be visited.
e. Specific dates of the visits.
f. Purpose of visit.

2. International conferences: Regardless of whether access to classified information is to be required, all letters of nomination for international conferences under the auspices of the Department of State shall include a statement that the nominees have been cleared by appropriate authority and are eligible as a minimum for access to information classified Secret.

3. Additional guidance: Further information on this subject is contained in OPNAV Instruction 5500.24, which should be reviewed by all prospective sponsoring commands prior to initiating visit notifications.

1413. DEPARTMENT OF THE NAVY SPONSORSHIP FOR VISITS OF FOREIGN NATIONALS INTO THE UNITED STATES

1. This article is applicable where the talents of outstanding foreign nationals are required by naval activities on an unclassified basis only and for a limited period. Because of the inherent possibility of espionage and fraud, the decision in each case as to whether the Department of the Navy will sponsor any foreign national shall not be made without prior reference to the head of a bureau or office of the Navy Department. The Chief of Naval Operations (Director of Naval Intelligence) should be consulted when desired and in all doubtful cases.

2. Interested naval activities may make discreet inquiries and preliminary examinations for the purpose of determining the desirability of sponsoring the visit of foreign nationals on unclassified projects within the United States. When a naval activity determines from a technical viewpoint that the visit of a foreign national is desirable, the following information relating to him shall be provided to the head of the appropriate bureau or office of the Navy Department:

a. Present full name of individual.
b. Other names previously or currently used.
c. Nationality.
d. Previous or current dual nationalities.
e. Date and place of birth.
f. Permanent addresses, and any previous U. S. addresses.
g. Names and residences of any relatives residing in the United States.
h. Purpose of sponsorship.
i. Special qualifications.
j. Present or prospective address in the U. S.
k. Length of time involved.
l. Sponsoring U. S. Navy or Marine Corps command (if other than the originator of the letter or message containing the above information).

3. After the head of the bureau or office concerned determines if the prospective visitor is acceptable, the interested naval activity will be notified as to whether or not sponsorship of the individual into the United States for the specified purpose is approved.

4. In exceptional circumstances, where time does not permit the completion of the procedure outlined above, the head of a bureau or office of the Navy Department is authorized to approve interim sponsorship. This may only be done following compilation of all information required in paragraph 2 above, and should be requested only in those instances where a change in plans or lack of notice prevents compliance with normal procedures.

Section 3
CLASSIFIED VISITS

1414. VISIT CLEARANCES

1. Visits to activities of the Naval Establishment by persons who will have access to classified information shall be processed in accordance with the requirements of Table C and article 1415 below. A visitor will be considered to have "access" to classified information when he is permitted to gain knowledge of such information through observation or discussion. This term is also interpreted to mean that a visitor will have access when classified information is exposed in such a manner in the space being visited, or enroute to the space to be visited, that he will gain knowledge through observation alone.

2. The column headings in Table C below are explained as follows:

a. Column 1, Category of Visitor—The "category of visitor" is as described in article 1403.

b. Column 2, Application Made By—This column sets forth the person designated to initiate the request for the visit clearance. Applications shall be made by letter or, if time does not allow, by message. They shall be submitted sufficiently in advance to permit necessary arrangements to be made. The entries under Column 2 are *not* exclusive but show rather the normal, expected originator of classified visit applications.

c. Column 3, To—This column specifies the cognizant officer to whom the application for visit clearance shall be addressed and who shall normally approve or disapprove the visit.

d. Column 4, Information Required—Certain information is required before final approval can be given. (Refer to article 1415.)

3. Commanders of activities of the Naval Establishment, who receive requests for visits requiring access to classified information by persons or under circumstances which do not fall within the categories covered in article 1403 and Table C, should refer the matter to appropriate higher authority or to the Chief of Naval Operations. As much of the information shown in article 1415 as is available, as well as pertinent recommendations, should be included.

1415. INFORMATION REQUIRED WITH VISIT REQUESTS

1. General. Applications for visits to activities of the Department of the Navy involving access to classified information shall be submitted in accordance with Table C above in sufficient time to allow evaluation by the command to be visited; the applications shall include the following information concerning the proposed visitor:

a. Name in full, rank, title and position.

b. Nationality, date and place of birth (submit only if a foreign national or an immigrant alien; in case of an immigrant alien, furnish also Alien Registration Number).

c. Employer or sponsor, if other than the originator of the visit application.

d. Name and address of activity to be visited, if other than the addressee of the visit application.

e. Date, time and duration of proposed visit.

f. Purpose of visit in detail, including estimated degree of access required.

g. Security clearance status of visitor and clearing agency.

h. Where appropriate, names of persons to be visited.

i. Whenever practicable, naval activities requesting approval or clearances for visits to other naval activities shall include the phrase "Reply only if negative" in the request and will assume that approval or clearance is granted unless otherwise advised.

2. Visits of Contractor Personnel. Department of Defense contractors desiring to have an employee visit an activity of the Naval Establishment involving access to classified information have been instructed to address a request in writing directly to the commanding officer of the activity to be visited.

TABLE C

Column 1	Column 2	Column 3	Column 4
Category of visitor	*Application made by*	*To*	*Information required*
One Alfa	No formal visit requirements are needed, but each person is responsible for complete compliance with the letter and spirit of article 0902.		
One Bravo	Commanding Officer of visitor	Commanding officer of activity to be visited	See Art. 1415.1
One Charlie	Appropriate official of the contracting facility	do	See Art. 1415.2
One Delta	Appropriate official of the Government agency involved	do	See Art. 1415.1
Two Alfa	Military attache or mission of foreign country concerned	CNO (DNI)	do
Two Bravo	Chief of mission (ambassador, minister, etc.) of foreign country concerned	do	do
Two Charlie	Administrative senior of business or activity	do	do
Three Alfa	Military attache or mission of foreign country concerned	do	do
Three Bravo	Chief of mission of foreign country concerned	do	do
Three Charlie	Commanding officer of visitor or appropriate official of the contracting facility	do	See Art. 1415.1 or 1415.2
Three Delta	Chief of mission of foreign country concerned	do	See Art. 1415.1

a. The contractor's request will contain the following information:

(1) Name and address of contractor requesting visit.

(2) Name and address of ship or station to be visited.

(3) Name in full and title of the person to be visited, if known.

(4) Name in full of contractor's employee, including title or position, for whom visit is requested.

(5) Citizenship of employee. (If immigrant alien, alien registration number, date and place of birth will be included.)

(6) Date (or dates) of requested visit (or visits).

(7) Purpose of and justification for visit (or visits) in detail. If a contract is involved, contract number, name and address of the military contracting activity will be furnished.

(8) Name and address of cognizant security office. (Telephone number, if known.)

(9) Contractor's certification as to degree, date and issuing military authority of "Letter of Notification of Facility Security Clearance" (DD Form 562) establishing the contractor's facility clearance.

(10) Contractor's certification of employee's current clearance status including degree, date and issuing authority. (In this regard, cleared contractors are themselves authorized to issue Confidential clearances to their own employees.)

b. On receipt of a contractor visit request as set forth above, the commanding officer of a naval activity may at his own discretion:

(1) Approve or disapprove the visit on the basis of the information provided, notifying the contractor accordingly; or if desired,

(2) Request that the contractor furnish additional information in order to evaluate more fully the original visit request. Approve or disapprove the visit request upon the basis of the additional information furnished, notifying the contractor accordingly.

(3) In lieu of the action outlined in subparagraph (2) above, the commanding officer may request (1) the information desired directly from the cognizant security office; (2) the Chief, Industrial and Personnel Security Group (8576), Fort Holabird, Baltimore 19, Maryland (Attn: Central Index File), to verify the clearance status of the individual and/or of the contractor; or (3) the military contracting activity to justify the visit as appropriate without referral to the contractor. Approval or disapproval of the visit will then be made on the basis of the additional information, the contractor being notified accordingly.

c. After visit relationships have been established, the commanding officer of the activity and the contractor may mutually arrange for future visits on a continuing basis. Final approval for such visits remains the prerogative of the commanding officer of the military activity.

d. Final approval of a visit is the prerogative of the commanding officer of the activity to be visited.

e. Cleared Department of Defense contractors have been authorized to grant their U. S. citizen employees access to DOD Confidential classified information without a DOD issued security clearance. These clearances are called "contractor-granted Confidential clearances". The Office of the Secretary of Defense has determined that such clearances are valid in connection with visits to military activities. Neither the Central Index File nor the cognizant security office of the contractor will be able to verify clearances of this type.

3. Visits to AEC Facilities. Requests for visits to facilities of the Atomic Energy Commission, including visits to joint AEC-DOD projects, shall be made as set forth in OPNAV Instruction 5510.3E or subsequent revisions.

1416. IDENTIFICATION

Any visitor who is authorized access to classified information must present adequate identification at the time of the visit. Commanding officers shall not permit access to classified information until they are satisfied as to the identity of the visitor.

1417. RELEASE OF CLASSIFIED DOCUMENTS TO VISITORS

Those visitors falling into the categories which must be approved by Chief of Naval Operations are normally approved for access to classified information for discussion and/or visual inspection only. Classified documents shall not be released to the visitor (s) for permanent retention unless such release is specifically authorized in the letter or message of approval.

1418. DEPARTMENT OF THE NAVY SPONSORSHIP OF CLASSIFIED VISITS TO FOREIGN COUNTRIES

1. When a naval activity proposes to sponsor visits of persons to foreign countries involving access to or discussion of classified information, that activity shall insure that nominees are reliable and trustworthy and that they have been properly cleared by competent authority to handle classified information of the security classification categories involved in the visit. This clearance shall be based on investigative requirements contained in Chapter 15. If classified Department of the Navy information is to be discussed with foreigners, prior authority for such discussions must be obtained from the Chief of Naval Operations (Director of Naval Intelligence).

Visit notifications shall be made as required in article 1412.1 above with the following additional information required:

g. Degree of security clearance held by individual.

h. Security clearance required. Only that degree of security clearance required to accomplish the purpose of the visit will be indicated here. Visit notifications shall delineate the specific items of information, and the classifications thereof, that may be discussed. Whenever applicable, the specific information that may be discussed with foreigners and that which may be discussed with U. S. military activities overseas shall be specified.

In addition all prospective sponsoring commands should review OPNAV Instruction 5500.24 or subsequent revisions prior to initiating visit notifications.

1419. DEPARTMENT OF THE NAVY SPONSORSHIP OF CLASSIFIED VISITS BY FOREIGN NATIONALS

1. When a naval activity proposes to sponsor a visit of a foreign national into the United States, or to a U. S. activity wherever located, and when such a visit will involve disclosure of classified information, the provisions set forth in article 1413, modified as indicated below, apply:

a. Application for approval shall be made in all cases to the Chief of Naval Operations (Director of Naval Intelligence) except in cases where authority has been separately delegated.

b. Application shall indicate the degree of clearance issued by the individual's government.

c. The prospective sponsoring command shall include in the application a certification that the visit is for the national benefit of the United States.

Chapter 15*

PERSONNEL SECURITY INVESTIGATIONS AND CLEARANCES FOR ACCESS TO CLASSIFIED INFORMATION

Section 1

PERSONNEL SECURITY INVESTIGATIONS

1501. RESPONSIBILITY

1. The Chief of Naval Operations (Director of Naval Intelligence), when requested by competent authority, shall be responsible for conducting security investigations of the following:

   a. Military and civilian personnel of the Naval Establishment.

   b. Private contractors and contractors' employees requiring access to classified information. (Refer to the Armed Forces Industrial Security Regulation, OPNAV Instruction 5540.8A or subsequent revisions.)

2. The Chief of Naval Operations (Director of Naval Intelligence) may initiate investigations which are essential to the security of the Naval Establishment.

3. It is the exclusive responsibility of the Chief of Naval Operations (Director of Naval Intelligence) to maintain liaison with other activities having investigative functions, particularly the Army, the Air Force, and the Federal Bureau of Investigation. Within the naval districts such liaison shall be maintained by the district intelligence officers.

1502. TYPES OF PERSONNEL SECURITY INVESTIGATIONS

1. Personnel security investigations are of two types:

   a. National Agency Check.

   b. Background Investigation.

2. National Agency Check:

   a. A National Agency Check consists of the investigation of records and files of the following agencies, as appropriate:

      (1) Federal Bureau of Investigation (FBI). The Headquarters files (criminal and subversive) shall be checked in every case. The FBI fingerprint files shall be checked in addition to subversive files. A properly completed non-criminal-type fingerprint card shall be submitted with each request (OPNAV Form 5510–2).

      (2) Office of Naval Intelligence, Department of the Navy (ONI), shall be checked in all cases.

      (3) Assistant Chief of Staff, Intelligence, Department of the Army, shall be checked when the individual is or has been in the Army or when he is or has been a civilian employee of the Department of the Army.

      (4) Office of Special Investigations, the Inspector General, USAF, Department of the Air Force (OSI), shall be checked when the individual is or has been in the Air Force or when he is or has been a civilian

*The provisions of this chapter relate only to the investigative and clearance requirements for access to classified information and have no bearing on the investigative requirements for employment of civilian personnel within the Naval Establishment or the acceptance of personnel for the naval service. Requirements relating thereto are contained in appropriate instructions issued by the Bureau of Naval Personnel, the Office of Industrial Relations, Commandant of the Marine Corps, or higher authority.

employee of the Department of the Air Force.

(5) Civil Service Commission (CSC) shall be checked on all persons who are or have been civilian employees of the United States Government.

(6) Immigration and Naturalization Service (INS) shall be checked in all cases in which the individual is an alien in the United States, an immigrant alien, or naturalized citizen.

(7) Central Index Personnel and Facility Security File shall be checked as determined by the Chief of Naval Operations (Director of Naval Intelligence).

(8) Bureau of Naval Personnel and/or Headquarters, U. S. Marine Corps, files shall be checked on each person who is or who has been a member of either service. In the case of Coast Guard Personnel, or personnel with Merchant Marine background, the files of the U. S. Coast Guard will also be checked.

(9) Other agencies shall be checked when pertinent to the purpose for which the investigation is being conducted. Chief of Naval Operations (Director of Naval Intelligence) shall determine when such other agencies should be checked.

b. The "record check and inquiry" conducted by the Civil Service Commission under Executive Order 9835 may be accepted as the equivalent of the National Agency Check plus written inquiries conducted by the Civil Service Commission under Executive Order 10450. Either check may be accepted for clearance purposes within the Naval Establishment with respect to civilian employees when the individual has been continuously in the employ of the Executive Branch of the Government since the completion of such investigation or there has been no break in the individual's employment longer than 90 days.

c. In the event derogatory or questionable information concerning an individual is disclosed by a National Agency Check, the inquiry will be extended as necessary to obtain such additional information as may be required as a basis upon which to grant or deny clearance.

3. Background Investigation:

A Background Investigation which is conducted for clearance purposes is designed to develop information as to whether the access to classified information by the person being investigated is clearly consistent with the interest of national security. It shall make inquiry into the pertinent facts bearing on the loyalty, integrity, and reputation of the individual. It will normally cover the period of his life from 1 January 1937 to the date of the investigation or from the date of his 18th birthday whichever is the shorter period. When derogatory information is developed in the course of any investigation the investigation shall be extended to any part of the individual's life necessary to support or discount the allegations. A Background Investigation comprises the following essential elements:

a. National Agency Check.

b. Birth Records.—The individual's date and place of birth shall be verified through schools, employment or other records examined during the investigation. Only if a discrepancy appears need vital statistics records be examined to establish the individual's correct date and place of birth.

c. Education.—Attendance at last school or college shall be verified except that verification of attendance at primary schools is not required in any circumstance; neither is verification of attendance at secondary schools prior to 1937 required. (Results of attendance at Service Schools will as a rule appear in the individual's service record and need not be confirmed.) In addition to examining school records persons in a position to know the individual's activities while in attendance should be interviewed, if available.

d. Employment.—The records of present and former employers shall be examined to verify the period of employment and efficiency record. Former employers and co-workers shall be interviewed, if available, to ascertain the loyalty, character, and reputation of the subject.

e. References.—The majority of the individual's references shall be interviewed. Interviews shall also be had with individuals (not relatives or former employers) who have knowledge of the subject's background and activities, but who are not given as references by the subject.

f. Neighborhood investigations.—These inquiries will be conducted when deemed necessary or expedient in substantiating or disproving derogatory information.

g. Criminal record.—The records of police departments and other law-enforcement agencies in the vicinities where subject has resided or been employed for substantial periods shall be checked.

h. Military service.—The service of subject in the Armed Forces and type of discharge shall be verified.

i. Foreign connections.—Any connections subject has had with foreigners in the United States or abroad are important and shall be reported. The extent and purpose of any such connections shall be ascertained as well as the relationship of the subject to foreign persons or organizations.

j. Citizenship status.—In all cases the citizenship status of the subject shall be established.

(1) United States citizens. (See subparagraph b above.)

(2) Immigrant aliens.—The records of the Immigration and Naturalization Service, Washington, D. C., shall be searched to verify date and place of birth, legal entry into the United States and to ascertain whether, and when, the individual has indicated an intention to become a citizen of the United States.

(3) Naturalized citizens.—The naturalization and date and place of birth shall be verified through records of the appropriate United States district court. If the place of naturalization cannot be determined, Immigration and Naturalization Service records, Washington, D. C., shall be examined.

k. Foreign travel.—If the subject has traveled outside the United States except in military or naval service, the State Department records shall be checked to determine reasons for such travel. If such travel occurred after 1 July 1946, records of the Central Intelligence Agency (CIA) shall also be checked.

l. Credit Record.—Whenever necessary credit agencies and/or credit references will be checked.

m. Organizations.—During the course of the investigation, as set forth above, and by examination of personal history statements and other records examined, efforts shall be made to determine if subject has:

"Membership in, or affiliation or sympathetic association with, any foreign or domestic organization, association, movement, group, or combination of persons, which is totalitarian, Fascist, Communist, or subversive, or which has adopted a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States, or which seek to alter the form of government of the United States by unconstitutional means." (Section 8(a) (5), E. O. 10450.)

Section 2

PERSONNEL SECURITY CLEARANCES

1503. INTERIM AND FINAL CLEARANCES

1. A personnel security clearance is an administrative determination that an individual is eligible, from a security standpoint, for access to classified information of the same or lower category as the clearance being granted. Security clearances are of two types:

a. Final clearance—one granted upon completion of all investigative requirements as set forth in this chapter.

b. Interim clearance—a determination of temporary eligibility for access to classified information based on the lesser investigative requirement as set forth in this chapter. An interim clearance shall be issued *only* when it is clearly established that the delay while waiting for the completion of the investigation required for a final clearance would be harmful to the national interest. Procedures to effect a final clearance shall be initiated simultaneously with the initiation of the procedures for an interim clearance.

2. If, upon review by the clearing authority of the Statement of Personal History (DD Form 398), it is apparent that the full investigative requirements for the category of clearance requested cannot be completed, an interim clearance shall not be granted, nor shall the investigation be initiated.

1504. GRANTING AND RECORDING CLEARANCES

1. It is the responsibility of competent authority (normally the commander or administrative senior in the chain of command) to insure that eligible personnel (military or civilians, including consultants, part-time employees and civilians paid from non-appropriated funds) under their jurisdiction are granted security clearances in accordance with the requirements of this chapter, prior to granting such personnel access to classified information. Such clearances (final and interim) shall be evidenced in each instance by the issuance of a Certificate of Clearance (OPNAV Form 5521–429), except as provided in paragraph 5 below.

2. Such Certificates of Clearance shall be made a matter of record and a permanent part of the subject's qualification jacket, service record, civilian personnel folder, or other appropriate record held by the command to which he is attached. When final clearances are granted to naval or Marine Corps personnel, the original Certificate of Clearance shall be forwarded to the Chief of Naval Personnel or to the Commandant of the Marine Corps (Code AO2), as appropriate, for insertion in personnel records.

3. Cryptographic clearances shall be indicated on Certificates of Clearance.

4. The original and all copies of Certificates of Clearance shall be signed by the commanding officer or his delegated representative (see Article 1510.1) and the ship or station seal or official seal of the U. S. Marine Corps, as appropriate, affixed.

5. Certificates of Clearance need not be executed for military and civilian personnel authorized to handle Confidential information unless the basis for authorization is a Background Investigation or a National Agency Check.

6. Certificates of Clearance or any other "certificate" form shall not be released to the subjects thereof, nor retained by them if previously released. This does not preclude military personnel from carrying their Service Records or Qualification Jackets containing such certificates when so directed or the inclusion of a statement of the clearance status in travel orders of military or civilian personnel.

7. A Certificate of Clearance does not in itself constitute authority for access to classified information. It is a determination of eligibility for access. Classified information is made available to appropriately cleared individuals only when a "need to know" is clearly established.

1505. CLEARANCE CRITERIA

1. Personnel authorized access to classified information must be:

a. Of unquestionable loyalty, integrity, and trustworthiness.

b. Of excellent character and of such habits and associations as to cast no doubt upon their discretion or good judgment in the handling of classified information.

2. Access to classified information shall be granted only when it has been determined that such access is clearly consistent with the interests of national security.

3. The activities and associations listed below may be the basis for denial or termination of clearance, but they are of varying degrees of seriousness. Therefore, the ultimate determination of whether clearance should be granted, denied or terminated must be an overall common-sense one, based on all available information concerning the following:

a. Commission of any act of sabotage, espionage, treason or sedition, or attempts thereat or

preparation therefor, or conspiring with or abiding or abetting another to commit or attempt to commit any act of sabotage, espionage, treason or sedition.

b. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests are inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

c. Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

d. Membership in, or affiliation or sympathetic association with, any foreign or domestic organization, association, movement, group, or combination of persons which is totalitarian, Fascist, Communist, or subversive, or which has adopted, or shows, a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights, under the Constitution of the United States, or which seeks to alter the form of government of the United States by unconstitutional means. (An organization, movement, or group, officially designated by the Attorney General of the United States to be totalitarian, Fascist, Communist, or subversive, to advocate or approve forcible or violent denial of Constitutional rights, or to seek alteration of the form of government of the United States by unconstitutional means, shall be presumed to be of a character thus designated until the contrary be established.)

e. Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

f. Failure or refusal to sign a loyalty certificate, or pleading protection of the Fifth Amendment or of Article 31, Uniform Code of Military Justice, in refusing to completely answer questions contained in required security forms or personal history statements; pleading protection of the Fifth Amendment or of Article 31, Uniform Code of Military Justice, or otherwise failing or refusing to answer any pertinent question propounded in the course of an official investigation, interrogation, or examination, conducted for the purpose of ascertaining the existence or extent, or both, of conduct of the nature described in a through e above and g through m below.

g. Participation in the activities of an organization established as a "front" for an organization referred to in d above, when his personal views were sympathetic to the subversive purposes of such organization.

h. Participation in the activities of an organization with knowledge that it had been infiltrated by members of subversive groups under circumstances indicating that the individual was a part of, or sympathetic to, the infiltrating element or sympathetic to its purposes.

i. Participation in the activities of an organization, referred to in d above, in a capacity where he should reasonably have had knowledge of the subversive aims or purposes of the organization.

j. Sympathetic association with a member or members of an organization referred to in d above, or sympathetic interest in totalitarian, Fascist, Communist, or similar subversive movements.

k. Currently maintaining a close continuing association with a person who has engaged in activities or associations of the type referred to in a through i above. A close continuing association may be considered to exist if the individual lives at the same premises as, frequently visits, or frequently communicates with such person.

l. Close continuing association of the type described in k above, even though later separated by distance, if the circumstances indicate that renewal of the association is probable.

m. Any facts, other than as set forth in n through s below, which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of national security. Among matters which should be considered in this category would be the presence of a spouse, parent, brother, sister, or offspring in a nation, a satellite thereof, or an occupied area thereof, whose interests are inimical to the interests of the United States.

n. Willful violation or disregard of security regulations.

o. Intentional unauthorized disclosure to any person of classified information, or of other information disclosure of which is prohibited by law.

p. Any deliberate misrepresentation, falsification, or omission of material fact.

q. Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.

r. Acts of a reckless, irresponsible or wanton nature which indicate such poor judgment and instability as to suggest that the individual might disclose security information to unauthorized persons or otherwise assist such persons, whether deliberately or inadvertently, in activities inimical to the security of the United States.

s. All other behavior, activities, or associations which tend to show that the person is not reliable or trustworthy.

t. Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the individual, with due regard to the transient or continuing effect of the illness and the medical findings in such case.

1506. INVESTIGATIVE REQUIREMENTS FOR CLEARANCES FOR U. S. CITIZENS WITHIN THE NAVAL ESTABLISHMENT

No U. S. citizen in the Naval Establishment (Regular and Reserve military personnel and civilians) shall be authorized access to classified information unless granted a clearance in accordance with the criteria of article 1505 and on the basis of the following investigative requirements:

1. TOP SECRET

   a. Final clearance.

      (1) Military personnel:

         (a) *Background Investigation, or

         (b) National Agency Check, PLUS continuous honorable active duty as a member of the Armed Forces or a combination of such active duty and civilian employment in the Government service on a continuous basis for a minimum of 10 consecutive years (with no break greater than 90 days) immediately preceding the date of the current investigation. (The NAC referred to above may have been conducted at any time during the 10 year period but subsequent to 14 September 1950. The phrase "current investigation" means the review of the records being conducted to determine the present clearance eligibility prior to granting the anticipated Top Secret clearance.), or

         (c) When the individual occupies a specific office in the Naval Establishment to which he has been appointed by the President by and with the advice and consent of the Senate.

      (2) Civilian personnel:

         (a) *Background Investigation, or

*When geographic and political situations prevent the full completion of a Background Investigation and the individual's services are required in the interest of national security, the Chief of Naval Operations (Director of Naval Intelligence) will render an opinion on the adequacy of the investigation to base a clearance decision or to grant "limited access authorization" for specific tasks or projects. In requesting such evaluation, the clearing authority will provide full details as to the need for the individual's services.

(b) When the individual occupies a specific office in the Naval Establishment to which he has been appointed by the President by and with the advice and consent of the Senate.

b. Interim clearance.

(1) Military personnel:

(a) National Agency Check, or

(b) Continuous honorable active duty as a member of the Armed Forces or a combination of such active duty and civilian employment in Government service on a continuous basis for a minimum of 5 consecutive years (with no break greater than 90 days) immediately preceding the date of the current investigation, plus

1. Check of ONI Case History files, and Bureau of Naval Personnel or Headquarters, U. S. Marine Corps files. These checks are made by ONI as part of a National Agency Check and the request therefor must be accompanied by the forms necessary for final clearance. These checks other than as part of the National Agency Check should only be requested in extremely urgent cases.

(2) Civilian personnel:

(a) National Agency check, except that individuals occupying sensitive-critical positions under the conditions of NCPI 29.7-6a(2) may be granted an interim clearance only under urgent circumstances.

2. Secret.

a. Final clearance.

(1) Military personnel:

(a) National Agency Check.

(2) Civilian personnel:

(a) Satisfactory completion of the National Agency Check and Written Inquiries conducted by the Civil Service Commission under Executive Order 10450 or satisfactory completion of "record check and inquiry" conducted by the Civil Service Commission under Executive Order 9835; except that a Background Investigation is required for employees occupying sensitive-critical positions as defined in NCPI 29.7-2j.

b. Interim clearance.

(1) Military personnel:

(a) Check of ONI Case History files, and Bureau of Naval Personnel or Headquarters, U. S. Marine Corps files. These checks are made by the Office of Naval Intelligence as part of the National Agency Check required for final clearance and the request therefor must be accompanied by the forms necessary for final clearance. These checks other than as part of the National Agency Check should only be requested in extremely urgent cases.

(2) Civilian personnel:

(a) National Agency Check.

(b) When an individual occupies a sensitive non-critical position under emergency conditions as set forth in NCPI 29.7-5a, he may be granted an interim clearance provided the personal history forms (SF 85 or DD 398), personnel records of the employing activity and the investigative records of the District Intelligence Office contain no derogatory information concerning the individual.

3. CONFIDENTIAL (INCLUDING CONFIDENTIAL—MODIFIED HANDLING AUTHORIZED)

a. Final clearance.

(1) Military personnel:

(a) Formal investigation is not required provided the personnel or other records immediately available to the command issuing the clearance contain no derogatory information concerning the individual.

(2) Civilian personnel:

(a) Same as requirements for final Secret clearance.

b. Interim clearance.

(1) Military personnel:

(a) None required.

(2) Civilian Personnel.

(a) Same as requirements for interim Secret clearance.

4. Duration of Validity of Security Investigations. A satisfactory investigation (Background Investigation, National Agency Check, or National Agency Check plus Written inquiries) having been once completed on an individual shall remain valid and may serve as the basis for the issue of future security clearances (appropriate to the scope of the investigation as prescribed in paragraphs 1–3 above) except:

a. When derogatory information concerning the individual becomes available indicating a need to reopen the investigation, or

b. When a particularly sensitive assignment is subject to special clearance criteria beyond the requirements of this chapter, or

c. When an individual's honorable active duty, active status in the Naval or Marine Corps Reserve, or civilian employment in the government service, or a combination thereof, has been interrupted for a period greater than 90 days. (When a retired officer, regular or reserve, has been assigned a mobilization billet in a currently effective War Plans List his release from active duty will not be considered a break in service.)

1507. INVESTIGATION REQUIREMENTS FOR CLEARANCES FOR IMMIGRANT ALIENS WITHIN THE NAVAL ESTABLISHMENT

No immigrant alien (See Article 0224) in the Naval Establishment may be authorized access to any category of classified information unless granted a final clearance on the basis of a *Background Investigation. In addition an immigrant alien to be eligible for a security clearance shall have formally declared his intent to become a U. S. citizen before a naturalization court by executing Naturalization Form N-315. The following additional requirements shall apply:

1. The investigation must cover the period from at least 1 January 1937, regardless of the individual's age.

2. Interim clearances shall not be granted to immigrant aliens. In the event that the delay for the completion of the investigation required for a final clearance would be harmful to the national interest, the Chief of Naval Operations (Director of Naval Intelligence) may, upon specific request from the command, authorize access for specific tasks or projects. Requests must clearly establish the harm to the national interest which would result from the delay and must specifically set forth the tasks or projects upon which the immigrant alien is to be utilized.

3. Following completion of the residence requirements for naturalization, the clearing authority shall ensure that the immigrant alien has in fact been naturalized. If the necessary action has not been accomplished within one year following completion of residence requirements, the immigrant alien's clearance shall be revoked, provided however that if the delay is due to causes beyond the control of the immigrant alien a reasonable additional delay may be authorized. For security clearances purposes, an immigrant alien whose clearance is revoked in compliance with this paragraph shall be considered to have reverted to foreign national status and article 1508 shall apply.

1508. EMPLOYMENT OF FOREIGN NATIONALS (OTHER THAN IMMIGRANT ALIENS) ON U. S. NAVY CLASSIFIED INFORMATION WITHIN THE NAVAL ESTABLISHMENT AND NAVAL CONTRACTORS' FACILITIES

1. Permission to utilize foreign nationals in any position, both military and civilian, either in the Naval Establishment or in private facilities, involving access to Navy classified information shall be granted only in cases of absolute necessity and for

*When geographic and political situations prevent the full completion of a Background Investigation and the individual's services are required in the interest of national security, the Chief of Naval Operations (Director of Naval Intelligence) will render an opinion on the adequacy of the investigation to base a clearance decision or to grant "limited access authorization" for specific tasks or projects. In requesting such evaluation, the clearing authority will provide full details as to the need for the individual's services.

specific tasks or projects. Permission shall be conditional upon the completion of a Background Investigation or such investigation as in the opinion of the Chief of Naval Operations (Director of Naval Intelligence) is sufficiently complete and reliable to form a basis for determining whether utilization of the foreign national is clearly consistent with the interest of National Security.

2. A case of absolute necessity shall be considered to have been established only when it is clearly shown that the individual's services are of such unique quality and character as to be unobtainable elsewhere and of such plain importance to the work upon which he is to be engaged that, if his services are not obtained, the work cannot proceed or will be seriously delayed or impaired to the extent that the national defense will directly suffer.

3. Since authorization for access to Navy classified information requires approval by the Chief of Naval Operations (Director of Naval Intelligence) in all instances where a foreign national is involved, interested naval activities (procuring activities in the case of contractors' employees) must initially request and receive permission to utilize the individual's services prior to requesting the Background Investigation. In submitting such requests, the information required in article 1413 shall be furnished, in addition to the justification for absolute necessity. In the case of contractors' employees, a completed Immigrant Alien Questionnaire (DD Form 49) shall also be submitted in addition to the information set forth in article 1413.

4. Activities of the Department of the Navy shall not accept personnel security clearances of foreign nationals granted by other U. S. Government agencies for visits, conferences, or other purposes, until a detailed justification of the absolute necessity for granting such foreign nationals access to naval classified information has been presented to and approved by the Chief of Naval Operations (Director of Naval Intelligence).

5. Access to Top Secret defense information may be granted to foreign nationals only upon the specific authorization of the Secretary of the Navy. Requests therefor will be forwarded via the Chief of Naval Operations (Director of Naval Intelligence).

1509. INVESTIGATION REQUIREMENTS FOR CONTRACTOR PERSONNEL

Refer to the Armed Forces Industrial Security Regulation (OPNAV Instruction 5540.8A or subsequent revisions).

1510. INVESTIGATIONS AND CLEARANCES FOR PERSONS ISSUING SECURITY CLEARANCES, SERVING ON PERSONNEL SECURITY BOARDS, OR INVOLVED IN SERVICE EDUCATION PROGRAMS

Although access to classified information may not be required for the performance of their duties, the below listed categories of personnel shall receive investigations as indicated:

1. Any person authorized to issue personnel security clearances shall have been the subject of an investigation meeting the requirements for a final Top Secret clearance.

2. Any person selected to serve with a board, committee, or other group responsible for adjudicating personnel security cases shall have been the subject of a favorable Background Investigation prior to his assignment, except that military personnel who have been granted a final Top Secret clearance in accordance with the provisions of Article 1506.1.a.(1) (b) above, and on whom a Background Investigation has been initiated, may be selected for service on military personnel security boards.

3. Any person selected for duties in connection with programs involving the education and orientation of service personnel shall have been the subject of a favorable National Agency Check prior to his assignment.

1511. CRYPTOGRAPHIC PERSONNEL SECURITY CLEARANCES

Personnel engaged in duties involving cryptographic information shall be cleared in accordance with instructions issued by the Chief of Naval Operations (Director, Naval Communications). (See OPNAV Instruction 5510.37A or subsequent revisions.)

1512. INVESTIGATIONS AND CLEARANCES FOR ACCESS TO RESTRICTED DATA

1. "Q" clearances are not required for individuals in the Naval Establishment requiring access to RESTRICTED DATA, provided the individuals

have been cleared for access to classified information at least equal to the classification category of the RESTRICTED DATA involved.

2. A "Q" clearance issued by the Atomic Energy Commission shall not be considered per se as an authoritative basis for automatically granting a personnel security clearance. However, after the request for investigation is submitted in accordance with article 1513, the investigation data upon which the "Q" clearance was based will be utilized in the processing of the current investigation.

3. The Atomic Energy Commission (AEC) grants two types of personnel security clearances, "L" and "Q" for access to classified information including RESTRICTED DATA to its employees and to its contractors' and consultants' employees. An "L" clearance is granted on the basis of a completed satisfactory National Agency Check; a "Q" clearance is granted on the basis of a completed satisfactory full field (background) investigation. Personnel granted "L" clearances are authorized access by the AEC to classified information at the Confidential level including Restricted Data; those granted "Q" clearances are considered eligible by the AEC for information through the Top Secret level including Restricted Data, although actual dissemination is governed by a strict need-to-know policy. Further, Atomic Energy Commission personnel and their contractors' and consultants' employees visiting installations of the Department of Defense or of DOD contractors are required by AEC regulations to have specific certification of their eligibility and need for the desired level of classified information. (In the case of AEC contractors' and consultants' employees, this certification will be made by the Manager of Operations administering the contract.) Accordingly, AEC-granted clearances will be given the following recognition for visit purposes:

a. A currently effective "L" clearance, in the case of employees of the Atomic Energy Commission and of its contractors and consultants, may be accepted as the basis for granting access to Confidential information including Restricted Data.

b. A currently effective "Q" clearance may be accepted as the basis for granting access to classified information through the Secret level including Restricted Data.

c. A currently effective "Q" clearance may be accepted as the basis for granting access to classified information through the Top Secret level including Restricted Data, *provided* the Atomic Energy Commission has authorized the individual concerned to have access to Top Secret and so indicates.

d. It should be noted that the Atomic Energy Commission also issues an "LX" and "QX" clearance. These clearances are issued to contractor employees who are working on an "access permit". The access permits are issued under separate laws and have no connection with the Department of Defense. The "LX" and "QX" cleared people are not permitted by AEC regulations to release classified information to the Department of Defense nor are the "LX" or "QX" cleared people recognized by the Department of Defense as being eligible to receive Department of Defense classified information.

1513. REQUESTS FOR PERSONNEL INVESTIGATIONS

1. Investigations of military personnel and civilians employed by the Naval Establishment shall be made by Naval Intelligence, upon request. Activities within a naval district or river command shall submit requests for investigations to the naval district or river command intelligence officer. All other activities shall submit requests to the Chief of Naval Operations (Director of Naval Intelligence). Requests for such investigations shall be initiated by submission of a properly executed "Request for Investigation for Personnel Security Clearance," OPNAV Form 5520-1. Parts 3 and 4 of the completed form shall be placed in the subject's personnel jacket to prevent duplication of investigative work in the event of transfer of the individual. Requests for a Background Investigation shall be accompanied by a properly executed Statement of Personal History (DD Form 398), in quadruplicate, an Agency Check Request (OPNAV Form 5510-397), and a Fingerprint Card (OPNAV Form 5510-2. Requests for a National Agency Check shall be accompanied by OPNAV Form

5510–397, a Fingerprint Card (OPNAV Form 5510–2), and a properly executed Statement of Personal History (DD Form 398). Incomplete or improperly executed forms will not be processed and will be returned to the originator for resubmission. In this connection it is desired to point out that fingerprints should be taken by qualified personnel.

2. Cancellation. If an investigation is in a pending status and an individual is released from duty, is discharged, resigns or is transferred to duties or employment not requiring a clearance, the activity shall promptly cancel the investigation using OPNAV Form 5520–1.

1514. RECIPROCAL ACCEPTANCE OF PREVIOUS INVESTIGATIONS AND CLEARANCES

1. In order to avoid the repetitious filing of Personal History Statements and the time and expense of multiple investigations, it is highly desirable that commanding officers accept from each other and from responsible authorities within the Executive Branch of the Government the following:

a. The results of previous investigations.

b. Existing clearances granted by competent authority on standards equivalent to those required in this chapter. In this connection all personnel security clearances granted under the authority of any agency of the Executive Branch of the Government, except as expressly forbidden in article 1508.4, are considered to meet the standards in this chapter (see also article 1512.3). This paragraph is particularly applicable to visitors, whose clearance remains in force while on temporary additional duty, i.e., so long as they are not *permanently* detached from their clearing command.

c. Previous clearances granted by competent authority within the Executive Branch of the Government are considered to meet the standards in this chapter. Acceptance of such previous clearances, as in the case of a person currently reporting for duty to a command, does not mean that a new Certificate of Clearance need not be issued; it does mean that its issuance normally should be based mainly on the presence in the individual's personnel or service record of a Certificate of Clearance which, except for the fact of his permanent detachment from his last duty station or place of employment, would still be valid. In this connection see article 1506.4.

2. The ultimate authority for granting clearance, accepting clearances on a reciprocal basis and authorizing access to classified information rests with the commanding officer who is responsible for the security of the information or material within his command. The commanding officer may request an individual's investigative record from the Office of Naval Intelligence or the appropriate District Intelligence Office before granting clearances or authorizing access to classified information if he feels that a review of the material is desirable.

1515. DENIAL OR TERMINATION OF CLEARANCE

1. Denial or termination of clearances of personnel of the Naval Establishment who do not or no longer meet the general requirements of unquestionable loyalty, integrity, trustworthiness, or excellent character (See article 1505) shall be made a matter of record of the activity concerned and shall be reported with full particulars pertaining thereto, as follows:

a. Military Personnel:

(1) To the Chief of Naval Personnel, to the Commandant of the Marine Corps as appropriate, and

(2) To the Director of Naval Intelligence, and

(3) To the naval district or river command intelligence officer, in the case of activities located within a naval district or river command.

b. Civilian Personnel:

(1) To the office maintaining the employee's personnel record, and

(2) To the Chief of Industrial Relations, and

(3) To the Director of Naval Intelligence, and

(4) To the naval district or river command intelligence officer in the case of naval

activities located within a naval district or river command.

In addition to the foregoing, wherever a clearance is terminated, an appropriate notation (cancellation) shall be made on the Certificate of Clearance (OPNAV Form 5521–429) indicating thereon the authority for the termination. (It should be noted that the above requirements are in addition to those of article 0619, which are to be complied with in every case.)

2. Clearances should be cancelled when there remains no present need for clearance and no need in the foreseeable future is anticipated. In such cases an appropriate notation should be placed on the Certificate of Clearance to the effect that the cancellation was due only to the fact that the individual's duties do not require clearance.

1516. COMBAT OPERATIONS

Under combat conditions or other military exigencies, competent authority may waive such provisions of this chapter as the circumstances may warrant.

Appendix A

PROCUREMENT OF FORMS

1.. FORMS UNDER MANAGEMENT CONTROL OF THE CHIEF OF NAVAL OPERATIONS

The forms listed below in this paragraph may be procured through the Navy Forms and Publications Supply System. Naval activities requiring these forms should submit DD Form 1149 (Requisition and Invoice/Shipping Documents), prepared in accordance with BUSANDA Manual Volume II Paragraph 22217, to the appropriate Supply Distribution Point indicated in Paragraph 27856 thereof.

Investigation Request for Personnel Security Clearance	OPNAV Form 5520–1
National Agency Check Request	OPNAV Form 5510–397
Fingerprint Card	OPNAV Form 5510–2
Statement of Personal History	DD 398
Certificate of Clearance for Handling Classified Matter	OPNAV Form 5521–429
Security Violation Notice Improperly Transmitted Material	OPNAV Form 5511–8
Record of Receipt	OPNAV Form 5511–10
Notice of Change in Classification	OPNAV Form 5511–11
Classified Matter Destruction Record	OPNAV Form 5511–12
Record of Disclosure	OPNAV Form 5511–13
Security Termination Statement	OPNAV Form 5511–14

Appendix B

Pertinent Extracts From The ATOMIC ENERGY ACT OF 1954 (Public Law 703 — 83d Congress)

"CHAPTER 1. DECLARATION, FINDINGS, AND PURPOSE

* * *

SECTION 3. Purpose. — It is the purpose of this Act to effectuate the policies set forth above by providing for —

a. a program of conducting, assisting, and fostering research and development in order to encourage maximum scientific and industrial progress;

b. a program for the dissemination of unclassified scientific and technical information and for the control, dissemination, and declassification of Restricted Data, subject to appropriate safeguards, so as to encourage scientific and industrial progress;

c. a program for Government control of the possession, use, and production of atomic energy and special nuclear material so directed as to make the maximum contribution to the common defense and security and the national welfare;

d. a program to encourage widespread participation in the development and utilization of atomic energy for peaceful purposes to the maximum extent consistent with the common defense and security and with the health and safety of the public;

e. a program of international cooperation to promote the common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit; and

f. a program of administration which will be consistent with the foregoing policies and programs, with international arrangements, and with agreements for cooperation, which will enable the Congress to be currently informed so as to take further legislative action as may be appropriate.

CHAPTER 2. DEFINITIONS

SECTION 11. Definitions.

* * *

r. The term "Restricted Data" means all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142.

* * *

CHAPTER 12. CONTROL OF INFORMATION

SECTION 141. Policy. — It shall be the policy of the Commission to control the dissemination and declassification of Restricted Data in such a manner as to assure the common defense and security. Consistent with such policy, the Commission shall be guided by the following principles:

a. Until effective and enforceable international safeguards against the use of atomic energy for destructive purposes have been established by an international arrangement, there shall be no exchange of Restricted Data with other nations except as authorized by section 144; and

b. The dissemination of scientific and technical information relating to atomic energy should be permitted and encouraged so as to provide that free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding and to enlarge the fund of technical information.

SECTION 142. Classification and Declassification of Restricted Data. —

a. The Commission shall from time to time determine the data, within the definition of Restricted Data, which can be published without undue risk to the common defense and security and shall thereupon cause such data to be declassified and removed from the category of Restricted Data.

b. The Commission shall maintain a continuous review of Restricted Data and of any Classification Guides issued for the guidance of those in the atomic energy program with respect to the areas of Restricted Data which have been declassified in order to determine which information may be declassified and removed from the category of Restricted Data without undue risk to the common defense and security.

c. In the case of Restricted Data which the Commission and the Department of Defense jointly determine to relate primarily to the military utilization of atomic weapons, the determination that such data may be published without constituting an unreasonable risk to the common defense and security shall be made by the Commission and the Department of Defense jointly, and if the Commission and the Department of Defense do not agree, the determination shall be made by the President.

d. The Commission shall remove from the Restricted Data category such data as the Commission and the Department of Defense jointly determine relates primarily to the military utilization of atomic weapons and which the Commission and Department of Defense jointly determine can be adequately safeguarded as defense information: *Provided, however,* That no such data so removed from the Restricted Data category shall be transmitted or otherwise made available to any nation or regional defense organization, while such data remains defense information, except pursuant to an agreement for cooperation entered into in accordance with subsection 144 b.

e. The Commission shall remove from the Restricted Data category such information concerning the atomic energy programs of other nations as the Commission and the Director of Central Intelligence jointly determine to be necessary to carry out the provisions of section 102 (d) of the National Security Act of 1947, as amended, and can be adequately safeguarded as defense information.

SECTION 143. Department of Defense Participation. — The Commission may authorize any of its employees, or employees of any contractor, prospective contractor, licensee or prospective licensee of the Commission to permit any employee of an agency of the Department of Defense or of its contractors, or any member of the Armed Forces to have access to Restricted Data required in the performance of his duties and so certified by the head of the appropriate agency of the Department of Defense or his designee: *Provided, however,* That the head of the appropriate agency of the Department of Defense or his designee has determined, in accordance with the established personnel security procedures and standards of such agency, that permitting the member or employee to have access to such Restricted Data will not endanger the common defense and security: *And provided further,* That the Secretary of Defense finds that the established personnel and other security procedures and standards of such agency are adequate and in reasonable conformity to the standards established by the Commission under section 145.

SECTION 144. International Cooperation. —

a. The President may authorize the Commission to cooperate with another nation and to communicate to that nation Restricted Data on —

(1) refining, purification, and subsequent treatment of source material;

(2) reactor development;

(3) production of special nuclear material;

(4) health and safety;

(5) industrial and other applications of atomic energy for peaceful purposes; and

(6) research and development relating to the foregoing: *Provided, however,* That no such cooperation shall involve the communication of Restricted Data relating to the design or fabrication of atomic weapons: *And provided further,* That the cooperation is undertaken pursuant to an agreement for cooperation entered into in accordance with section 123, or is undertaken pursuant to an agreement existing on the effective date of this Act.

b. The President may authorize the Department of Defense, with the assistance of the Commission, to cooperate with another nation or with a

regional defense organization to which the United States is a party, and to communicate to that nation or organization such Restricted Data as is necessary to —

(1) the development of defense plans;

(2) the training of personnel in the employment of and defense against atomic weapons; and

(3) the evaluation of the capabilities of potential enemies in the employment of atomic weapons, while such other nation or organization is participating with the United States pursuant to an international arrangement by substantial and material contributions to the mutual defense and security: *Provided, however,* That no such cooperation shall involve communication of Restricted Data relating to the design or fabrication of atomic weapons except with regard to external characteristics, including size, weight, and shape, yields and effects, and systems employed in the delivery or use thereof but not including any data in these categories unless in the joint judgment of the Commission and the Department of Defense such data will not reveal important information concerning the design or fabrication of the nuclear components of an atomic weapon: *And provided further,* That the cooperation is undertaken pursuant to an agreement entered into in accordance with section 123.

* * *

CHAPTER 18. ENFORCEMENT

SECTION 221. General Provisions. —

a. To protect against the unlawful dissemination of Restricted Data and to safeguard facilities, equipment, materials, and other property of the Commission, the President shall have authority to utilize the services of any Government agency to the extent he may deem necessary or desirable.

b. The Federal Bureau of Investigation of the Department of Justice shall investigate all alleged or suspected criminal violations of this Act.

c. No action shall be brought against any individual or person for any violation under this Act unless and until the Attorney General of the United States has advised the Commission with respect to such action and no such action shall be commenced except by the Attorney General of the United States: ***Provided, however,*** That no action shall be brought under sections 222, 223, 224, 225 or 226 except by the express direction of the Attorney General.

SECTION 222. Violation of Specific Sections. — Whoever willfully violates, attempts to violate, or conspires to violate, any provision of sections 57, 92, or 101, or whoever unlawfully interferes, attempts to interfere, or conspires to interfere with any recapture or entry under section 108, shall, upon conviction thereof, be punished by a fine of not more than $10,000 or by imprisonment for not more than five years, or both, except that whoever commits such an offense with intent to injure the United States or with intent to secure an advantage to any foreign nation shall, upon conviction thereof, be punished by death or imprisonment for life (but the penalty of death or imprisonment for life may be imposed only upon recommendation of the jury), or by a fine of not more than $20,000 or by imprisonment for not more than twenty years, or both.

SECTION 223. Violation of Sections Generally. — Whoever willfully violates, attempts to violate, or conspires to violate, any provision of this Act for which no penalty is specifically provided or of any regulation or order prescribed or issued under section 65 or subsections 161 b., i., or p. shall, upon conviction thereof, be punished by a fine of not more than $5,000 or by imprisonment for not more than two years, or both, except that whoever commits such an offense with intent to injure the United States or with intent to secure an advantage to any foreign nation, shall, upon conviction thereof, be punished by a fine of not more than $20,000 or by imprisonment for not more than twenty years, or both.

SECTION 224. Communication of Restricted Data. — Whoever, lawfully or unlawfully, having possession of, access to, control over, or being entrusted with any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data —

a. communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with intent to injure the United States or with intent to secure an advantage to any foreign nation, upon conviction

464175ms—58——13

thereof, shall be punished by death or imprisonment for life (but the penalty of death or imprisonment for life may be imposed only upon recommendation of the jury), or by a fine of not more than $20,000 or imprisonment for not more than twenty years, or both;

b. communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation, shall, upon conviction, be punished by a fine of not more than $10,000 or imprisonment for not more than ten years, or both.

SECTION 225. Receipt of Restricted Data. — Whoever, with intent to injure the United States or with intent to secure an advantage to any foreign nation, acquires, or attempts or conspires to acquire any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data shall, upon conviction thereof, be punished by death or imprisonment for life (but the penalty of death or imprisonment for life may be imposed only upon recommendation of the jury), or by a fine of not more than $20,000 or imprisonment for not more than twenty years, or both.

SECTION 226. Tampering with Restricted Data. — Whoever, with intent to injure the United States or with intent to secure an advantage to any foreign nation, removes, conceals, tampers with, alters, mutilates, or destroys any document, writing, sketch, photograph, plan, model, instrument, appliance, or note involving or incorporating Restricted Data and used by any individual or person in connection with the production of special nuclear material, or research or development relating to atomic energy, conducted by the United States, or financed in whole or in part by Federal funds, or conducted with the aid of special nuclear material, shall be punished by death or imprisonment for life (but the penalty of death or imprisonment for life may be imposed only upon recommendation of the jury), or by a fine of not more than $20,000 or imprisonment for not more than twenty years, or both.

SECTION 227. Disclosure of Restricted Data. — Whoever, being or having been an employee or member of the Commission, a member of the Armed Forces, an employee of any agency of the United States, or being or having been a contractor of the Commission or of an agency of the United States, or being or having been an employee of a contractor of the Commission or of an agency of the United States, or being or having been a licensee of the Commission, or being or having been an employee of a licensee of the Commission, knowingly communicates, or whoever conspires to communicate or to receive, any Restricted Data, knowing or having reason to believe that such data is Restricted Data, to any person not authorized to receive Restricted Data pursuant to the provisions of this Act or under rule or regulation of the Commission issued pursuant thereto, knowing or having reason to believe such person is not so authorized to receive Restricted Data shall, upon conviction thereof, be punishable by a fine of not more than $2,500.

SECTION 228. Statute of Limitations. — Except for a capital offense, no individual or person shall be prosecuted, tried, or punished for any offense prescribed or defined in sections 224 to 226, inclusive, of this Act unless the indictment is found or the information is instituted within ten years next after such offense shall have been committed.

SECTION 229. Other Laws. — Sections 224 to 228 shall not exclude the applicable provisions of any other laws.

SECTION 230. Injunction Proceedings. — Whenever in the judgment of the Commission any person has engaged or is about to engage in any acts or practices which constitute or will constitute a violation of any provision of this Act, or any regulation or order issued thereunder, the Attorney General on behalf of the United States may make application to the appropriate court for an order enjoining such acts or practices, or for an order enforcing compliance with such provision, and upon a showing by the Commission that such person has engaged or is about to engage in any such acts or practices, a permanent or temporary injunction, restraining order, or other order may be granted.

SECTION 231. Contempt Proceedings. — In case of failure or refusal to obey a subpoena served upon any person pursuant to subsection 161 c., the district court for any district in which such person is found

or resides or transacts business, upon application by the Attorney General on behalf of the United States, shall have jurisdiction to issue an order requiring such person to appear and give testimony or to appear and produce documents, or both, in accordance with the subpoena; and any failure to obey such order of the court may be punished by such court as a contempt thereof.

APPENDIX C

EXECUTIVE ORDER 10450
(With amendments E.O. 10491, E.O. 10531, E.O. 10548, and E.O. 10550, appended)

29 April 1953

(18 F. R. 2489)

SECURITY REQUIREMENTS FOR GOVERNMENT EMPLOYMENT

WHEREAS the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and

WHEREAS the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service:

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U. S. C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U. S.C. 632, et seq.); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U. S. C. 118 j); and the act of August 26, 1950, 64 Stat. 476 (5 U. S. C. 22-1, et seq.), and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

SECTION 1. In addition to the departments and agencies specified in the said act of August 26, 1950, and Executive Order No. 10237 of April 26, 1951, the provisions of that act shall apply to all other departments and agencies of the Government.

SECTION 2. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

SECTION 3. (a) The appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation. The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation: Provided, that upon request of the head of the department or agency concerned, the Civil Service Commission may, in its discretion, authorize such less investigation as may meet the requirements of the national security with respect to per-diem, intermittent, temporary, or

seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, there shall be conducted with respect to such person a full field investigation, or such less investigation as shall be sufficient to enable the head of the department or agency concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

(b) The head of any department or agency shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full field investigation has been conducted: Provided, that a person occupying a sensitive position at the time it is designated as such may continue to occupy such position pending the completion of a full field investigation, subject to the other provisions of this order: And provided further, that in case of emergency a sensitive position may be filled for a limited period by a person with respect to whom a full field preappointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

SECTION 4. The head of each department and agency shall review, or cause to be reviewed, the cases of all civilian officers and employees with respect to whom there has been conducted a full field investigation under Executive Order No. 9835 of March 21, 1947, and, after such further investigation as may be appropriate, shall re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, such of those cases as have not been adjudicated under a security standard commensurate with that established under this order.

SECTION 5. Whenever there is developed or received by any department or agency information indicating that the retention in employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his representative, who, after such investigation as may be appropriate, shall review, or cause to be reviewed, and, where necessary, re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, the case of such officer or employee.

SECTION 6. Should there develop at any stage of investigation information indicating that the employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, the head of the department or agency concerned or his representative shall immediately suspend the employment of the person involved if he deems such suspension necessary in the interests of national security and, following such investigation and review as he deems necessary, the head of the department or agency concerned shall terminate the employment of such suspended officer or employee whenever he shall determine such termination necessary or advisable in the interests of the national security, in accordance with the said act of August 26, 1950.

SECTION 7. Any person whose employment is suspended or terminated under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950, or pursuant to the said Executive Order No. 9835 or any other security or loyalty program relating to officers or employees of the Government, shall not be reinstated or restored to duty or reemployed in the same department or agency and shall not be reemployed in any other department or agency, unless the head of the department or agency concerned finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of the national security, which finding shall be made a part of the records of such department or agency: Provided, that no person whose employment has been terminated under such authority thereafter may be employed by any other department or agency except after a determination by the Civil Service Commission that such person is eligible for such employment.

SECTION 8. (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or

retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:

(1) Depending on the relation of the Government employment to the national security:

(i) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

(ii) Any deliberate misrepresentations, falsifications, or omissions of material facts.

(iii) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.

(iv) An adjudication of insanity, or treatment for serious mental or neurological disorder without satisfactory evidence of cure.

(v) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.

(2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefor, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(3) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or the alteration of the form of government of the United States by unconstitutional means.

(4) Advocacy of use of force or violence to overthrow the Government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

(5) Membership in, or affiliation or sympathetic association with, any foreign or domestic organization, association, movement, group, or combination of persons which is totalitarian, Fascist, Communist, or subversive, or which has adopted, or shows, a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the Constitution of the United States, or which seeks to alter the form of government of the United States by unconstitutional means.

(6) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(7) Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(b) The investigation of persons entering or employed in the competitive service shall primarily be the responsibility of the Civil Service Commission, except in cases in which the head of a department or agency assumes that responsibility pursuant to law or by agreement with the Commission. The Commission shall furnish a full investigative report to the department or agency concerned.

(c) The investigation of persons (including consultants, however employed), entering employment of, or employed by, the Government other than in the competitive service shall primarily be the responsibility of the employing department or agency. Departments and agencies without investigative facilities may use the investigative facilities of the Civil Service Commission, and other departments and agencies may use such facilities under agreement with the Commission.

(d) There shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information relating to any of the matters described in subdivisions (2) through (7) of subsection (a) of this section. In cases so referred to it, the Federal Bureau of Investigation shall make a full field investigation.

SECTION 9. (a) There shall be established and maintained in the Civil Service Commission a security-investigations index covering all persons

as to whom security investigations have been conducted by any department or agency of the Government under this order. The central index established and maintained by the Commission under Executive Order No. 9835 of March 21, 1947, shall be made a part of the security-investigations index. The security-investigations index shall contain the name of each person investigated, adequate identifying information concerning each such person, and a reference to each department and agency which has conducted an investigation concerning the person involved or has suspended or terminated the employment of such person under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950.

(b) The heads of all departments and agencies shall furnish promptly to the Civil Service Commission information appropriate for the establishment and maintenance of the security-investigation index.

(c) The reports and other investigative material and information developed by investigations conducted pursuant to any statute, order, or program described in section 7 of this order shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with the said act of August 26, 1950, as may be required for the efficient conduct of Government business.

SECTION 10. Nothing in this order shall be construed as eliminating or modifying in any way the requirement for any investigation or any determination as to security which may be required by law.

SECTION 11. On and after the effective date of this order the Loyalty Review Board established by Executive Order No. 9835 of March 21, 1947, shall not accept agency findings for review, upon appeal or otherwise. Appeals pending before the Loyalty Review Board on such date shall be heard to final determination in accordance with the provisions of the said Executive Order No. 9835, as amended. Agency determinations favorable to the officer or employee concerned pending before the Loyalty Review Board on such date shall be acted upon by such Board, and whenever the Board is not in agreement with such favorable determination the case shall be remanded to the department or agency concerned for determination in accordance with the standards and procedures established pursuant to this order. Cases pending before the regional loyalty boards of the Civil Service Commission on which hearings have not been initiated on such date shall be referred to the department or agency concerned. Cases being heard by regional loyalty boards on such date shall be heard to conclusion, and the determination of the board shall be forwarded to the head of the department or agency concerned: Provided, that if no specific department or agency is involved, the case shall be dismissed without prejudice to the applicant. Investigations pending in the Federal Bureau of Investigation or the Civil Service Commission on such date shall be completed, and the reports thereon shall be made to the appropriate department or agency.

SECTION 12. Executive Order No. 9835 of March 21, 1947, as amended, is hereby revoked. For the purposes described in section 11 hereof the Loyalty Review Board and the regional loyalty boards of the Civil Service Commission shall continue to exist and function for a period of one hundred and twenty days from the effective date of this order, and the Department of Justice shall continue to furnish the information described in paragraph 3 of Part III of the said Executive Order No. 9835, but directly to the head of each department and agency.

SECTION 13. The Attorney General is requested to render to the heads of departments and agencies such advice as may be requisite to enable them to establish and maintain an approprite employee-security program.

SECTION 14. (a) The Civil Service Commission, with the continuing advice and collaboration of representatives of such departments and agencies as the National Security Council may designate, shall make a continuing study of the manner in which

this order is being implemented by the departments and agencies of the Government for the purpose of determining:

(1) Deficiencies in the department and agency security programs established under this order which are inconsistent with the interests of, or directly or indirectly weaken, the national security.

(2) Tendencies in such programs to deny to individual employees fair, impartial, and equitable treatment at the hands of the Government, or rights under the Constitution and laws of the United States or this order.

Information affecting any department or agency developed or received during the course of such continuing study shall be furnished immediately to the head of the department or agency concerned. The Civil Service Commission shall report to the National Security Council, at least semiannually, on the results of such study, and shall recommend means to correct any such deficiencies or tendencies.

(b) All departments and agencies of the Government are directed to cooperate with the Civil Service Commission to facilitate the accomplishment of the responsibilities assigned to it by subsection (a) of this section.

SECTION 15. This order shall become effective thirty days after the date hereof.

DWIGHT D. EISENHOWER

THE WHITE HOUSE
April 27, 1953

(F. R. Doc. 53-3794; Filed, Apr. 27, 1953; 4:04 p.m.)

EXECUTIVE ORDER 10491

13 October 1953

(18 F. R. 6583)

AMENDMENT OF EXECUTIVE ORDER NO. 10450 OF APRIL 27, 1953, RELATING TO SECURITY REQUIREMENTS FOR GOVERNMENT EMPLOYMENT

By virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U.S.C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U.S.C. 632, et seq.); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U.S.C. 118j); and the act of August 26, 1950, 64 Stat. 476 (5 U.S.C. 22-1, et seq.), and as President of the United States, and finding such action necessary in the best interests of the national security, it is hereby ordered as follows:

Subsection (a) of section 8 of Executive Order No. 10450 of April 27, 1953, relating to security requirements for Government employment, is hereby amended by adding thereto at the end thereof paragraph (8) as follows:

"(8) Refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of his alleged disloyalty or other misconduct."

DWIGHT D. EISENHOWER

The White House
October 13, 1953

EXECUTIVE ORDER 10531

27 May 1954

(19 F.R. 3069)

AMENDMENT OF EXECUTIVE ORDER NO. 10450 OF APRIL 27, 1953, AS AMENDED, RELATING TO SECURITY REQUIREMENTS FOR GOVERNMENT EMPLOYMENT

By virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U.S.C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U.S.C. 632 et seq.); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U.S.C. 118j); and the act of August 26, 1950, 64

Stat. 476 (5 U.S.C. 22–1, et seq.), and as President of the United States, and finding such action necessary in the best interests of the national security, it is hereby ordered as follows:

Subsection (d) of section 8 of Executive Order No. 10450 of April 27, 1953, as amended by Executive Order No. 10491 of October 13, 1953, relating to security requirements for Government employment is hereby amended by striking out after the words "subdivisions (2)" the words "through (7)" and substituting the words "through (8)" so that the last clause of the first sentence of that section will read as follows:

"or information relating to any of the matters described in subdivisions (2) through (8) of subsection (a) of this section."

DWIGHT D. EISENHOWER

The White House
May 27, 1954

EXECUTIVE ORDER 10548

2 August 1954

(19 F.R. 4871)

AMENDMENT OF EXECUTIVE ORDER NO. 10450 OF APRIL 27, 1953, AS AMENDED, RELATING TO SECURITY REQUIREMENTS FOR GOVERNMENT EMPLOYMENT

Subsection (a) (1) (iv) of section 8 of Executive Order No. 10450 of April 27, 1953, relating to security requirements for Government employment, is hereby amended to read as follows:

"(iv) Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case."

DWIGHT D. EISENHOWER

The White House
August 2, 1954

EXECUTIVE ORDER 10550

5 August 1954

(19 F.R. 4981)

AMENDMENT OF EXECUTIVE ORDER NO. 10450 OF APRIL 27, 1953, AS AMENDED, RELATING TO SECURITY REQUIREMENTS FOR GOVERNMENT EMPLOYMENT

Section 14 of Executive Order No. 10450 of April 27, 1953, relating to security requirements for Government employment, is hereby amended as follows:

1. The last sentence of subsection (a) thereof is amended to read:

"The Civil Service Commission shall report to the National Security Council, at least semiannually, on the results of such study, shall recommend means to correct any such deficiencies or tendencies, and shall inform the National Security Council immediately of any deficiency which is deemed to be of major importance."

2. The following subsection is added at the end thereof:

"(c) To assist the Civil Service Commission in discharging its responsibilities under this order, the head of each department and agency shall, as soon as possible and in no event later than ninety days after receipt of the final investigative report on a civilian officer or employee subject to a full field investigation under the provisions of this order, advise the Commission as to the action taken with respect to such officer or employee. The information furnished by the heads of departments and agencies pursuant to this section shall be included in the reports which the Civil Service Commission is required to submit to the National Security Council in accordance with subsection (a) of this section. Such reports shall set forth any deficiencies on the part of the heads of departments and agencies in taking timely action under this order, and shall mention specifically any instances of noncompliance with this subsection."

DWIGHT D. EISENHOWER

The White House
August 5, 1954

APPENDIX D

ESPIONAGE AND CENSORSHIP
(18 U. S. C., 1952 ed., 791–797)

SECTION 791. Scope of chapter.
792. Harboring or concealing persons.
793. Gathering, transmitting, or losing defense information.
794. Gathering or delivering defense information to aid foreign government.
795. Photographing and sketching defense installations.
796. Use of aircraft for photographing defense installations.
797. Publication and sale of photographs of defense installations.

SECTION 791. Scope of Chapter.—This chapter shall apply within the admiralty and maritime jurisdiction of the United States and on the high seas, as well as within the United States.

SECTION 792. Harboring or concealing persons.—Whoever harbors or conceals any person who he knows, or has reasonable grounds to believe or suspect, has committed, or is about to commit, an offense under section 793 or 794 of this title, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

SECTION 793. Gathering, transmitting, or losing defense information.—(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station, or other place connected with the national defense, owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions or other materials or instruments for use in time of war are being made, prepared, repaired, stowed or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose of aforesaid, and with like intent, or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose of aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan,

map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

SECTION 794. Gathering or delivering of defense information to aid foreign government.—

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be imprisoned not more than twenty years.

(b) Whoever violates subsection (a) in time of war shall be punished by death or by imprisonment for not more than thirty years.

(c) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the armed forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operation, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for not more than thirty years.

(d) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

SECTION 795. Photographing and sketching defense installations.—(a) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment

as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

(b) Whoever violates this section shall be fined not more than $1,000 or imprisoned not more than one year, or both.

SECTION 796. Use of aircraft for photographing defense installations.—Whoever uses or permits the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment, in violation of section 795 of this title, shall be fined not more than $1,000 or imprisoned not more than one year, or both.

SECTION 797. Publication and sale of photographs of defense installations.—On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title, whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp, or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined not more than $1,000 or imprisoned not more than one year, or both.

Appendix E

EXECUTIVE ORDER 10104
February 1, 1950
(15 F. R. 597)

DEFINING CERTAIN VITAL MILITARY AND NAVAL INSTALLATIONS AND EQUIPMENT AS REQUIRING PROTECTION AGAINST THE GENERAL DISSEMINATION OF INFORMATION RELATIVE THERETO

Whereas section 795 of title 18 of the United States Code provides:

"(a) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.

"(b) Whoever violates this section shall be fined not more than $1,000 or imprisoned not more than one year, or both.";

And whereas section 797 of title 18 of the United States Code provides:

"On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under Section 795 of this title, whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer of the military or naval post, camp, or station concerned, or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined not more than $1,000 or imprisoned not more than one year, or both.":

Now, therefore, by virtue of the authority vested in me by the foregoing statutory provisions, and in the interests of national defense, I hereby define the following as vital military and naval installations or equipment requiring protection against the general dissemination of information relative thereto:

1. All military, naval, or air-force installations and equipment which are now classified, designated, or marked under the authority or at the direction of the President, the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, or the Secretary of the Air Force as "top secret", "secret", or "confidential", and all military, naval, or air-force installations and equipment which may hereafter be so classified, designated, or marked with the approval or at the direction of the President, and located within:

(a) Any military, naval, or air-force reservation, post, arsenal, proving ground, range, mine field, camp, base, airfield, fort, yard, station, district or area.

(b) Any defensive sea area heretofore established by Executive Order and not subsequently discontinued by Executive Order, and any defensive sea area hereafter established under authority of section 2152 of title 18 of the United States Code.

(c) Any airspace reservation heretofore or hereafter established under authority of section 4 of the Air Commerce Act of 1926 (44 Stat. 570;

49 U.S.C. 174) except the air-space reservation established by Executive Order No. 10092 of December 17, 1949.

(d) Any naval harbor closed to foreign vessels.

(e) Any area required for fleet purposes.

(f) Any commercial establishment engaged in the development or manufacture of classified military or naval arms, munitions, equipment, designs, ships, aircraft, or vessels for the United States Army, Navy, or Air Force.

2. All military, naval, or air-force aircraft, weapons, ammunition, vehicles, ships, vessels, instruments, engines, manufacturing machinery, tools, devices, or any other equipment whatsoever, in the possession of the Army, Navy, or Air Force or in the course of experimentation, development, manufacture, or delivery for the Army, Navy, or Air Force which are now classified, designated, or marked under the authority or at the direction of the President, the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, or the Secretary of the Air Force as "top secret", "secret", or "confidential", and all such articles, materials, or equipment which may hereafter be so classified, designated, or marked with the approval or at the direction of the President.

3. All official military, naval, or air-force books, pamphlets, documents, reports, maps, charts, plans, designs, models, drawings, photographs, contracts, or specifications which are now marked under the authority or at the direction of the President, the Secretary of Defense, the Secretary of the Army, the Secretary of the Navy, or the Secretary of the Air Force as "top secret", "secret", or "confidential", and all such articles or equipment which may hereafter be so marked with the approval or at the direction of the President.

This order supersedes Executive Order No. 8381 of March 22, 1940, entitled "Defining Certain Vital Military and Naval Installations and Equipment".

HARRY S. TRUMAN.

The White House,
February 1, 1950.

Appendix F

CRYPTOGRAPHIC SYSTEMS
Title 18 U.S.C. 1952 ed., Sec. 798

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) Concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) Concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) Concerning the communication intelligence activities of the United States or any foreign government; or

(4) Obtained by the process of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof (Added Oct. 31, 1951, ch. 655, sec. 24 (a), 65 Stat. 719.)

Appendix G

EMPLOYMENT SUSPENSION
Act of August 6, 1950

(P.L. 733, 81st Cong.; c. 803, 64 Stat. 476; 5 U.S.C., 1952 ed., 22–1)

To protect the national security of the United States by permitting the summary suspension of employment of civilian officers and employees of various departments and agencies of the Government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That, notwithstanding the provisions of section 6 of the Act of August 24, 1912 (37 Stat. 555), as amended (5 U. S. C. 652), or the provisions of any other law, the Secretary of State; Secretary of Commerce; Attorney General; the Secretary of Defense; the Secretary of the Army; the Secretary of the Navy; the Secretary of the Air Force; the Secretary of the Treasury; Atomic Energy Commission, the Chairman, National Security Resources Board; or the Director, National Advisory Committee for Aeronautics, may, in his absolute discretion and when deemed necessary in the interest of national security, suspend, without pay, any civilian officer or employee of the Department of State (including the Foreign Service of the United States), Department of Commerce, Department of Justice, Department of Defense, Department of the Army, Department of the Navy, Department of the Air Force, Coast Guard, Atomic Energy Commission, National Security Resources Board, or National Advisory Committee for Aeronautics, respectively, or of their several field services: Provided, That to the extent that such agency head determines that the interests of the national security permit, the employee concerned shall be notified of the reasons for his suspension and within thirty days after such notification any such person shall have an opportunity to submit any statements or affidavits to the official designated by the head of the agency concerned to show why he should be reinstated or restored to duty. The agency head concerned may, following such investigation and review as he deems necessary, terminate the employment of such suspended civilian officer or employee whenever he shall determine such termination necessary or advisable in the interest of the national security of the United States, and such determination by the agency head concerned shall be conclusive and final: Provided further, That any employee having a permanent or indefinite appointment, and having completed his probationary or trial period, who is a citizen of the United States whose employment is suspended under the authority of this Act, shall be given after his suspension and before his employment is terminated under the authority of this Act, (1) a written statement within thirty days after his suspension of the charges against him, which shall be subject to amendment within thirty days thereafter and which shall be stated as specifically as security considerations permit; (2) an opportunity within thirty days thereafter (plus an additional thirty days if the charges are amended) to answer such charges and to submit affidavits; (3) a hearing, at the employee's request, by a duly constituted agency authority for this purpose; (4) a review of his case by the agency head, or some official designated by him, before a decision adverse to the employee is made final; and (5) a written statement of the decision of the agency head: Provided further, That any person whose employment is so suspended or terminated under the authority of this Act may, in the discretion of the agency head concerned, be reinstated or restored to duty, and if so reinstated or restored shall be allowed compensation for all or any part of the period of such suspension or termination in an amount not to exceed the difference between the amount such person would normally have earned during the period of such suspension or termination, at the rate he was receiving on the date of suspension or termination, as appropriate,

and the interim net earnings of such person: Provided further, That the termination of employment herein provided shall not affect the right of such officer or employee to seek or accept employment in any other department or agency of the Government: Provided further, That the head of any department or agency considering the appointment of any person whose employment has been terminated under the provisions of this Act may make such appointment only after consultation with the Civil Service Commission, which agency shall have the authority at the written request of either the head of such agency or such employee to determine whether any such person is eligible for employment by any other agency or department of the Government.

SECTION 2. Nothing herein contained shall impair the powers vested in the Atomic Energy Commission by the Atomic Energy Act of 1946 or the requirements of section 12 of that Act that adequate provision be made for administrative review of any determination to dismiss any employee of said Commission.

SECTION 3. The provision of this Act shall apply to such other departments and agencies of the Government as the President may, from time to time, deem necessary in the best interests of national security. If any departments or agencies are included by the President, he shall so report to the Committees on Armed Services of the Congress.

SECTION 4. Section 3 of the Act of December 17, 1942 (56 Stat. 1053), and section 104 of the Act of July 20, 1949 (P.L. 179, 81st Cong., and section 630 of the Act of October 29, 1949 (P.L. 434, 81st Cong.), are hereby repealed.

Appendix H

INTERNAL SECURITY ACT OF 1950
SECTIONS 4 and 21

(P.L. 831, 81st Cong.; c. 1024, 64 Stat. 991; 50 U.S.C., 1952 ed., Sup. IV, 783, 797)

SECTION 4. (a) It shall be unlawful for any person knowingly to combine, conspire, or agree with any other person to perform any act which would substantially contribute to the establishment within the United States of a totalitarian dictatorship, as defined in paragraph (15) of section 3 of this title, the direction and control of which is to be vested in, or exercised by or under the domination or control of, any foreign government, foreign organization, or foreign individual: Provided however, That this subsection shall not apply to the proposal of a constitutional amendment.

(b) It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 3 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

(c) It shall be unlawful for any agent or representative of any foreign government, or any officer or member of any Communist organization as defined in paragraph (5) of section 3 of this title, knowingly to obtain or receive, or attempt to obtain or receive, directly or indirectly, from any officer or employee of the United States or of any department or agency thereof or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, unless special authorization for such communication shall first have been obtained from the head of the department, agency, or corporation having custody of or control over such information.

(d) Any person who violates any provision of this section shall, upon conviction thereof, be punished by a fine of not more than $10,000, or imprisonment for not more than ten years, or by both such fine and such imprisonment, and shall, moreover, be thereafter ineligible to hold any office, or place of honor, profit, or trust created by the Constitution or laws of the United States.

(e) Any person may be prosecuted, tried, and punished for any violation of this section at any time within ten years after the commission of such offense, notwithstanding the provisions of any other statute of limitations: Provided, That if at the time of the commission of the offense such person is an officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, such person may be prosecuted, tried, and punished for any violation of this section at any time within ten years after such

person has ceased to be employed as such officer or employee.

(f) Neither the holding of office nor membership in any Communist organization by any person shall constitute per se a violation of subsection (a) or subsection (c) of this section or of any other criminal statute. The fact of the registration of any person under section 7 or section 8 of this title as any officer or member of any Communist organization shall not be received in evidence against such person in any prosecution for any alleged violation of subsection (a) or subsection (c) of this section or for any alleged violation of any other criminal statute.

SECURITY REGULATIONS AND ORDERS AND PENALTY FOR VIOLATION THEREOF

SECTION 21. (a) Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the Secretary of Defense, or by the Director of the National Advisory Committee for Aeronautics, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, water-front facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the Department of Defense, any Department or agency of which said Department consists, or any officer or employee of said Department or agency, or of the National Advisory Committee for Aeronautics or any officer or employee thereof, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse or other unsatisfactory conditions thereon, or the ingress thereto or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident or by enemy action, sabotage or other subversive actions, shall be guilty of a misdemeanor and upon conviction thereof shall be liable to a fine of not to exceed $5,000 or to imprisonment for not more than one year, or both.

(b) Every such regulation or order shall be posted in conspicuous and appropriate places.

Appendix I

PROTECTIVE ALARM SYSTEMS

1. Purpose.

Protective alarm systems provide an electrical and mechanical means of detecting and announcing proximity or intrusion which endangers or may endanger the security of an activity or its components. Protective alarm systems are utilized to accomplish one or more of the following purposes:

a. To permit more economical and efficient use of manpower by substitution of mobile responding guard units for larger numbers of fixed guards and/or patrols.

b. To take the place of other necessary elements of physical security which cannot be used because of building layout, safety regulations, operating requirements, appearance, cost, or other reasons.

c. To provide additional controls at vital areas as insurance against human or mechanical failure.

2. Types of Alarm Systems.

a. Central Station.—A central station alarm system is one in which the operation of electrical protection circuits and devices is automatically signalled to a central station which has trained guards and operators in attendance at all times. The central station monitors the signal end of the alarm system, provides the response to a signal, and supervises the functioning of the system.

b. Local.—A local alarm system is one in which the protective circuits and devices are connected to a visual and/or audible signal element which is located at or in the immediate vicinity of the protected activity or component, and which is responded to by guard personnel in the immediate vicinity.

3. Elements of Alarm Systems.—There is on the market a variety of alarm equipment based on different principles of operation and designed to meet various requirements. There are, however, three fundamental elements required in all alarm systems. These elements are:

a. A detection device or series of such devices. Most common among these are:

(1) Foils, screens, and traps which are damaged or disturbed by penetration. (Usually used for protection of doors, windows, ducts, and non-substantial walls or partitions.)

(2) Photo-electric systems, whereby interruption of a virtually invisible beam of light is detected.

(3) Electromagnetic wave or electronic system whereby entrance of an intruder into the field of the system is detected.

(4) Microphonic devices which detect sound and vibration.

(5) Pneumatic detectors of various types which serve the same purpose as mechanical and electrical detectors.

(6) Thermal detectors, actuated by exceeding a predetermined temperature limit or rate of rise.

b. Electrical circuits and radio for transmitting signals from the protected area to the signal apparatus.

c. An alarm or signal apparatus which will announce by audible and/or visual means any activity which the system is designed to detect.

4. Classification of Alarm Systems.

a. The Underwriters' Laboratories, Inc., have established Grade A and Grade B classifications for both central station and local alarm systems. These same designations are used herein.

b. Details of requirements for each type and grade of alarm systems are set forth in Underwriters' Laboratories, Inc., publications "Standard for Central Station Burglar Alarm Systems", "Standard for Local Burglar Alarm Systems", and "Standard for Installation, Classification, and Certification of Burglar Alarm Systems."

5. Use of Alarm Systems.

The use of alarms in the protective program of an activity may be required in certain instances because of the critical importance of a facility and, in other instances, because of situations and conditions pertaining to the location and/or the layout of the activity. In some instances, their use may be justified as a more economical and efficient substitute for other necessary protective elements. In determining whether the use of alarms in an

activity's protective program is essential or advisable, the various conditions and situations peculiar to the activity will, of course, affect the ultimate decision.

a. Location and Layout.—In certain cases due to restrictions imposed by location, layout, or construction, alarms are necessary to take the place of the more usual protective elements such as fences, lighting, patrols, etc. Included in this group are:

(1) Activities which because of proximity to adjacent structures, activities, or property lines, require the use of alarms in lieu of physical barriers to limited or exclusion areas;

(2) Activities which are difficult or impossible to effectively guard due to terrain conditions, personnel hazards, or atmospheric conditions and where other types of protection are not effective or practicable.

(3) Activities or components thereof which are small or remote areas requiring more than safe and lock protection but not justifying a full-time guard.

b. Other Considerations.—Alarm systems, because of their cost, are justified only where their use results in a commensurate reduction or replacement of other necessary protective elements without loss of protective effectiveness. The objective of such use, in most instances, is to reduce the number of guards otherwise required. In determining the advisability of substituting alarms for other protective elements, a careful comparison of relative cost is essential. This should include consideration of the initial cost of the system as well as recurring service and maintenance charges. In this connection, it should be borne in mind that alarm systems have little salvage value and consequently the longevity of the activity being protected is an important consideration. Obviously, alarms would hardly be justified at a temporary facility or activity of short duration.

6. Design and Operating Standards.

To afford the required degree of protection and be acceptable as a protective unit, alarm installations should meet the following minimum requirements:

a. The system should be so designed that the interval of time between the detection of activity and the achievement of the objective of such activity is sufficient to permit the application of necessary countermeasures.

b. Central Station systems should be specified where alarms are incorporated in the protective system for activities described in paragraph 5.a (3) and for all locations where guards are not continually in the immediate vicinity to pick up a local alarm signal and make adequate response.

c. Central Station alarm systems for activities should meet, as a minimum, the requirements of Grade B.

d. Local alarm systems should meet, as a minimum, the requirements established for Mercantile Premises Alarms, Grade B.

e. All material and equipment should have Underwriters' Laboratories approval where applicable for the purpose for which it is used.

f. All installations should be made in accordance with accepted Underwriters' Laboratories standards for burglar alarm systems.

7. Installation Safeguards.

a. It is apparent that knowledge of the details of a specific alarm installation may afford an individual a means of effectively by-passing the installation. Moreover, the accumulation of such knowledge in a questionable individual who has been employed on several installations presents a clear and present danger to our security structure.

b. Usually the original installation of protective alarm systems is accomplished by construction contract. Various elements are involved, among them: the contract document, specifications, detailed drawings, and the actual physical labor necessary to the installation of the device. Since all protective alarm devices in current use are sold on the open market, classification of the device itself is not appropriate. In many instances the general location of the device is not of a classified nature, though its presence should not be advertised in any case. The contract document itself may reflect only administrative details and nothing of a classified nature. This may be true also of the specifications involved in the contract.

c. However, in view of the discussion in subparagraph a. above, the detailed drawings of a particular installation should be classified and physical access to certain details of installation, knowledge of which would aid in circumventing an alarm system, must be restricted to cleared personnel.

d. Addressees shall be guided by the provisions of the Armed Forces Industrial Security Regulation, OPNAV Instruction 5540.8A, in processing

contracts for the installation, inspection or maintenance of alarm systems used to protect classified information. It may be noted that in the Armed Forces Industrial Security Regulation a classified contract is defined as any contract that requires access to classified information by the contractor or his employees in the performance of the contract.

e. The following particular regulations shall apply to contracts for the installation, inspection or maintenance of alarm systems used for the protection of classified information and to the various phases of their performance:

(1) The contract document itself, specifications, requisitions, and such related memoranda need not be classified unless they reflect such detail of installation or arrangement of circuits or alarms as would suggest the means for their circumvention.

(2) All drawings or sketches which reflect the details of a particular alarm system installation in such a manner as to suggest means for circumvention shall be classified Secret.

(3) Organizations utilized to install, inspect or maintain alarm systems for the protection of classified information shall have an active Secret facility clearance.

(4) All contractor personnel engaged in or having access to the installation, inspection or maintenance of such systems shall have a Secret clearance.

(5) Information relating to the precise location of an alarm system installation may or may not necessitate classification. This determination shall be made by the command involved, and shall be based upon the particular circumstances of the individual case.

Appendix J

SECURITY AREAS

1. Different activities involve different degrees of security interest depending upon their purpose and the nature of the work, information, and/or materials concerned. For similar reasons, different areas within an activity may have varying degrees of security importance. To meet this situation and, at the same time, facilitate operations and simplify the security system, requires the application of restrictions, controls, and protective measures commensurate with these varying degrees of security importance. In some cases, the entire area of an activity may have a uniform degree of security importance requiring only one level of restriction and control. In others, differences in degree of security importance will require further segregation or compartmentalization of certain activities.

2. To meet different levels of security sensitivity and provide for an effective and efficient basis for applying the varying degrees of restriction of access, control of movement, and type of protection required, three types of security areas have been established as follows:

a. Exclusion Area.—An exclusion area is one containing classified information which is of such nature that access to the area constitutes, for all practical purposes, access to such classified information.

b. Limited Area.—A limited area is defined as one containing classified information and in which area uncontrolled movement would permit access to such classified information; but within which area such access may be prevented by escort and other internal restrictions and controls.

c. Controlled Area.—A controlled area is defined as one adjacent to or encompassing limited or exclusion areas and within which area uncontrolled movement does not permit access to classified information, and which is designed for the principal purpose of providing administrative control, safety, and/or a buffer area of security restriction for limited or exclusion areas.

BASIC SECURITY MEASURES REQUIRED

1. Exclusion Areas.

The following basic security measures are required at all exclusion areas:

a. A clearly defined perimeter barrier.

b. A personnel identification and control system.

c. All points of ingress and egress are guarded.

d. Only persons whose duties actually require access and who have been granted appropriate security clearances shall be allowed into exclusion areas.

2. Limited Areas.

The following basic security measures are required at all limited areas:

a. A clearly defined perimeter barrier.

b. A personnel identification and control system.

c. All points of ingress and egress must be:

(1) Guarded, or

(2) Controlled by receptionists or other persons whose duties include check of identification, or

(3) Under automatic alarm protection.

d. All persons admitted to a limited area with freedom of movement within such area shall have appropriate security clearances. Persons who have not been cleared for access to the information contained within a limited area may, with appropriate approval, be admitted to such area, but in such instances they shall be so controlled by escort, attendants, and/or other security regulations as will prevent access to the classified information located within the area.

3. Controlled Areas.

The folowing basic security measures are required at a controlled area:

a. A clearly defined perimeter.

b. A personnel identification and control system.

c. Checking stations at all regularly used points of access at which identification may be checked.

d. Security and administrative arrangements for determining the need for access and method of approval for access to the area. Under normal conditions, approval for access to a controlled area will be based on operational need for access and adequate identification of the individual rather than on his security clearance status.

INDEX

Article No.

Access:
- definition ... 0201
- for destruction ... 0629
- personnel, to closed or open containers, value of control of ... Ch. 6, sec. 1, table A
- reports on personnel investigations, policy on ... App. C, sec. 9
- unauthorized, prevention ... 0614
- visitors', information required for ... 1413, 1415
- visitors', interpretation ... 1414

Accounting:
- category B messages ... 0611
- classified information held by personnel in travel status ... 0705
- classified information passed from watch to watch ... 0615
- Confidential information ... 0609
- destroyed material ... 0625
- publications distributed through RPS ... 0610
- Secret information ... 0608
- Top Secret information ... 0607, 0905
- Top Secret Restricted Data originated by AEC ... 0612

Accumulations of classified material, avoiding ... 0622

Addresses:
- containers for transmission ... 0710
- correct, sources of ... 0711

Advance security planning ... 0405

Advertising, commercial, policy on ... 1008

Adviser to photographers, provision for ... 1104

Aerial photographs and maps, classification and release ... 1106

Aerial reconnaissance, continuous cover, marking ... 0421

Aircraft, use for unauthorized photographing of defense installations prohibited ... App. D, sec. 796

Alarm systems:
- information on ... App. I
- security value ... Ch. 6, sec. 1, table A

Aliens (see Immigrant aliens)

ANAF, information of joint interest to, release policy ... 1004

Archives, transfer to ... 0618

Areas:
- guarding, security value ... Ch. 6, sec. 1, table A
- security, types of ... App. J
- surrounding, separately protected, value ... Ch. 6, sec. 1, table A
- working, care of ... 0616

Article No.

Armed Forces Courier Service:
classified information transmitted outside Continental Limits U. S. 0703
mail, reporting evidence of tampering with 0803
material authorized for 0709
Top Secret transmission within Continental Limits U. S. 0701
Arms, international traffic in, administration by State Department 0922
Army-Navy-Air Force, information of joint interest to, release policy 1004
Art work, original, marking 0421
Articles, publication 1009
Artists pictures, control 1109
Atomic Energy Act of 1954:
marking for identification of Restricted Data 0427, 0432
provisions ..... App. B
Atomic Energy Commission:
"L", "LX", "Q", "QX" clearances 1512
"Q" clearances 0903, 1512
Top Secret Restricted Data originated by, accounting for 0612
Authority to classify 0401
Automatic downgrading, marking for 0425

B

Back covers, marking classification 0421
Background investigation (see also Full field investigations; Personnel clearances):
requests for 1513
requirements 1502
Bank vaults, definition ..... Ch. 6, sec. 1, table A
Bars for ground-floor office windows 0616
Basis for security instructions 0104
Books:
marking classification 0421
publication of 1009
Bound documents:
definition 0202
regraded, marking 0426
Buildings:
heavily constructed, definition ..... Ch. 6, sec. 1, table A
lightly constructed, definition ..... Ch. 6, sec. 1, table A
Bulky material:
inspection of packages prior to transmission 0710
regraded documents, marking stocks of 0426
transmission 0708
Burn bags, stowage or destruction 0615
Burning method for destruction of classified material 0623

Article No.

C

Cameras:
naval personnel on ships or aircraft 1102
visitors', must be specifically authorized 1101
Canadian mail system, use allowed in certain areas 0703
Capital letters, use for marking classification 0423, 0427
Carbon sheets, destruction 0614, 0615
Categories (see also Messages):
classified material 0203, 0301
visitors 1403
Censorship:
personal, a fundamental duty 0909
personal mail 0912
Central Intelligence Agency:
Armed Forces Courier Service for material authorized by 0709
classification of titles of publications 0410
Central station alarm system, information on ..... App. I, 2a
Certain vital military and naval installations and equipment, definition ..... App. E, 1–3
Certificates:
classification review before transfer to stowage 0417
Clearance for Handling Classified Information 1504
destruction 0623, 0626
to be executed by personnel upon separation 0619
Chain receipts:
category B messages 0611
Top Secret material 0607, 0712
Charts, marking 0421
Cipher, definition of term ..... App. F
Cipher machines, stowage 0603
Circuits approved for transmission of Secret and Confidential 0911
Circulation control 0211
Civil courts, production of records for use in, policy 0917
Civil Service Commission:
determination of eligibility for employment after suspension or termination ..... App. C, sec. 7; App. G
investigations, acceptance for clearance purposes 1502
security-investigations index, furnishing information for ..... App. C, sec. 9
Claims against the United States, detrimental disclosures prohibited 0918
Classification (see also Reclassification):
alarm systems ..... App. I, 4
assignment according to content 0406
authority for original 0401
categories 0301
code words 0412
compilations 0406, 0407
derivative authority 0401

Article No.

Classification — Continued
documents referring to classified information 0406
equipment 0408
highest component determining factor 0407
letters of transmittal 0407
marking 0421
original authority 0401
records of court proceedings 0916
records of lock combinations 0605
review before transfer to stowage 0417
short title 0411
single, for each document 0407
titles or subjects 0409
Classification Guide 0204, 0404
Classified Information (see also Top Secret; Secret; Confidential):
accessibility for destruction 0629
accumulations, avoidance 0622
care after working hours 0615
care during emergencies 0617
care during working hours 0614
categories 0203
definition 0205
disclosure to foreign agents prohibited ..... App. H, sec. 4
disclosures outside Executive Branch, policy on 0923, 0925
dissemination responsibility 0901, 0902
individual responsibility for 0613
originated outside Department of Defense, dissemination 0904
protection by personnel in travel status 0705
received from foreign governments, marking 0431
transmission outside Continental Limits U. S. 0703
transmission outside Executive Branch, marking 0433
transmission within commands or specifically designated activities 0704
Classified Material Control Officer:
designation 0501
duties 0502
Classified Material, definition 0206
Classified Matter, definition 0207
Classifying, definition 0208
Clearance (see also Personnel clearance):
definition 0209
participants in conferences where disclosures are made 0928, 0929
persons issuing security clearances 1510
visitors 1414
witnesses for destruction of classified material 0623
Code:
definition of term ..... App. F
private, use in personal communications prohibited 0912

Article No.

Code — Continued
words, classification 0412
Collisions of ships, surveys prohibited in certain cases 0919
Color for classification marking 0423
Combination locks:
conventional, definition ..... Ch. 6, sec. 1, table A
manipulation-proof, definition ..... Ch. 6, sec. 1, table A
Combinations:
access for emergency destruction 0629
changing and recording 0605
Commanding officer, definition 0212
Commercial advertising policy 1008
Commercial photographers, review of photographs taken by 1103
Commercial proprietary information, policy on release 0924
Commercial proprietary material, marking 0428
Commercial transportation of bulky material 0708
Committees, congressional, testimony before 0914
Communication equipment, destruction 0626
Communication intelligence, definition ..... App. F
Communication material:
Armed Forces Courier Service for certain 0709
emergency destruction 0628
Communication security:
definition 0210
instructions 1302
responsibility for 1301
Communications (see also Mail; Telephone):
circuits approved for Secret and Confidential 0911
Compartmentalization 0211
Competent authority, definition 0212
Compilations, classifying and handling 0406, 0407
Composition tapes, making 0421
Compromise:
changing combinations or keys to stowage containers in case of 0605
declassification or downgrading not made on basis of 1005
definition 0213
disciplinary action in case of 0805
reporting 0801
Concealing violaters of Espionage and Censorship Act, penalties for ..... App. D, sec. 792
Conferences:
disclosure requests, information required to process 0929, 0930
disclosures to, policy on 0926, 0927
international, clearance of nominees for 1412
minutes of 0905
Navy sponsorship 0928–0931
physical security protection 0931

Article No.

Confidential:
accounting for ... 0609
authority to classify ... 0401
bulky material, transmission ... 0708
classification denotes vital military and naval installations and equipment ... App. E, 1-3
clearance, Naval Establishment personnel, U. S. citizens, investigative requirements ... 1506
definition and use ... 0304
destruction ... 0623
dissemination to Reserve personnel for training, policy on ... 0908
lettering used for marking ... 0423
preparation, printing, and reproduction ... 1204
stowage requirements evaluation graph ... Ch. 6, sec. 1, table B
transmission within Continental Limits U. S. ... 0702
Congressional committees, testimony before ... 0914
Containers (see also Stowage containers):
for transmission of classified material, preparation ... 0710
Continuous cover aerial reconnaissance, marking ... 0421
Contractor:
disclosures to ... 0924
photographs by, policy on ... 1102
Contractors' facilities:
employment of foreign nationals on classified information ... 1508
employment of immigrant aliens on classified information ... 1507
Control measures, limitations ... 0105
Control officers, classified material:
designation ... 0501
duties ... 0502
Control officers, Top Secret:
designation ... 0503
duties ... 0504
Controlled area, definition and requirements ... App. J
Conversations:
oral, personal censorship ... 0909
telephone, discussion of classified information prohibited ... 0909, 0910
Copies:
destruction ... 0618
marking assigned classification ... 0421
messages, categories A, AC and B, handling ... 1304
Top Secret, numbering ... 0420, 0607, 0906
Counterintelligence, definition ... 0215
Courier (see Armed Forces Courier Service)
Court-martial trials:
personnel responsible for loss, compromise, or unauthorized disclosure ... 0805
protection of classified information during ... 0916
Courts, civil, production of records for use in, policy ... 0917

Article No.

Cover pages, front and back, marking 0421
Cryptanalytic data, release policy 1007
Cryptographic material:
access or issuance to inactive reservists prohibited 0908
Armed Forces Courier Service for 0709
Certificate of Clearance for Handling 1504
emergency destruction 0628
loss, compromise, or unauthorized disclosure, reporting 0801
personnel clearances for 1511
registered, stowage 0603
transmission 0707
Cryptographic systems:
definition of terms ..... App. F
preventing disclosures concerning ..... App. F
use 1303
Cryptologic material, Armed Forces Courier Service for 0709
Customs inspection of classified material not permitted 0705

D

Death, recovery of classified information in case of 0621
Declassify (see also Downgrading):
definition 0216
Defense information (see Information)
Definitions (see specific subjects)
Derivative classification authority 0231
Desertion, recovery of classified material in cases of 0621
Desks with key locks, value ..... Ch. 6, sec. 1, table A
Destruction plan, emergency, maintenance 0627
Diplomatic pouch:
Armed Forces Courier Service for 0709
classified material transmitted outside Continental Limits U.S. 0703
Disciplinary action (see also Penalties):
for loss, compromise, or unauthorized disclosure 0805
Disclosure:
definition 0217
record forms, maintenance 0905
Documents (see also Bound documents; Unbound documents):
Atomic Energy Commission, return to originator in lieu of destruction 0612
classified, sale prohibited 1205
definition 0218
referring to classified information, classification 0406
release to visitors prohibited 1417
Downgrading:
automatic, marking for 0425
compromise or unauthorized publication not basis for 1005

Article No.

Downgrading — Continued
definition 0219
overclassified information 0413, 0414
technical equipment 0418
Drafts, preliminary, classification or destruction 0401, 0420, 0614, 0615
Drawings:
marking 0421
miscellaneous, control of 1109

E

Elements required in alarm system ..... App. I, sec. 3
Emergency:
care during 0617
destruction, accessibility 0629
destruction plan 0627
destruction priority 0628
Employment, Government:
determination of eligibility for, after suspension or termination ..... App. C, sec. 7; App. G
security requirements for ..... App. G
suspension or termination of civilians to protect national security ..... App. C, sec. 6; App. G
Enclosures, marking 0424
Endorsements, marking 0424
Envelopes, sealing and marking 0710
Equipment:
certificates of destruction for 0625
classification 0408
communication, destruction 0626
destruction 0624
military and naval, defining as vital ..... App. E, 1–3
special, marking 0422
technical, downgrading 0418
Escorts for visitors 1405, 1407
Espionage, reporting 0802
Espionage and Censorship Act:
marking classified material disseminated outside Executive Branch of Government 0433
provisions of ..... App. D
Evaluation graph, minimum levels of required stowage protection ..... 0602; Ch. 6, sec. 1, table B
Exclusion area, definition and requirements ..... App. J
Executive Order:
10104 ..... App. E
10450 ..... App. C
Extracts, control 0906
Extraordinary security measures for unusually sensitive operations 0912

Article No.

F

Files, classified papers relating to Top Secret documents 0420

Filing cabinets, steel:
- combination-lock, value ..... Ch. 6, sec. 1, table A
- key-lock, value ..... Ch. 6, sec. 1, table A

Film (see also Microfilm):
- motion-picture, marking 0421
- motion-picture, regraded, marking 0426
- training, changing security classification 0419
- training, contracts for 1105

Final clearance:
- definition 1503
- immigrant aliens, Naval Establishment and contractors' personnel, investigative requirements 1507
- Naval Establishment personnel, U. S. citizens, investigative requirements 1506

Fire alarms, stowage during 0617
Fire resistance of containers, value ..... Ch. 6, sec. 1, table A
For Official Use Only, definition 0220

Foreign countries, visits to, Navy sponsorship:
- classified visits 1418
- unclassified visits 1412

Foreign governments:
- classified material received from, marking 0431
- classified material to be released to, marking 0430
- definition ..... App. F
- disclosures to agents of prohibited ..... App. H, sec. 4
- gathering or delivering defense information to aid, penalties for ..... App. D, sec. 794
- mail systems, use prohibited except as specified 0703
- reports, reclassification 0414
- unauthorized disclosures to prohibited 0920

Foreign nationals:
- classified material not releasable to, marking 0429
- definition 0221
- employment on classified information, policy 1508
- training 0921
- unauthorized disclosures to prohibited 0920
- visits to U. S., Navy sponsorship of 1413, 1419

Foreign naval missions, requests for visits to ships 1410
Formerly Restricted Data 0305

Forms:
- disclosure record for Top Secret 0905
- new, requisitioning ..... App. A
- standard, requisitioning 0108

Front covers, marking 0421
Full field investigation, requirement for filling sensitive positions ..... App. C, sec. 3

Article No.

G

Graphic arts:
functions, application of security measures to 1202
industry, responsibility for protection of classified information 1203
Grilles for ground-floor office windows 0616
Ground-floor offices, precautions for protection 0616
Guarding, security value ..... Ch. 6, sec. 1, table A
Guards for shipments of bulky material 0708

H

Handling, definition of term 0223
Harboring persons, penalties for ..... App. D, sec. 792

I

Identification, visitors 1405
Immigrant aliens:
definition 0224
Naval Establishment and contractors' personnel, investigative requirements for clearance 1507
Inactive personnel, unauthorized disclosures to prohibited 0907, 0908
Indexes, marking 0421
Industrial proprietary information:
marking 0428
release policy 0924
Information:
defense, gathering, transmitting, or losing, penalties for ..... App. D, sec. 793–794
definition 0225
proprietary, commercial or industrial, marking 0428
proprietary, commercial or industrial, policy on release 0924
technical, definition 0241
Inner containers, addressing and marking 0710
Interim clearance:
definition and basis for issuance 1503
Naval Establishment personnel, U. S. citizens, investigative requirements 1506
not granted immigrant aliens in Naval Establishment 1507
Internal Security Act of 1950, sections 4 and 21 ..... App. H
International conferences, clearance of nominees for 1412
International documents, definition 0226
International traffic in arms, administration by State Department 0922
Inventory, semiannual, of AEC Top Secret documents 0612
Investigations (see also Personnel investigations):
loss, compromise, or unauthorized disclosure 0801

Article No.

J

Jettisoning for destruction of classified material 0624, 0629

K

Keys:
access for destruction 0629
changing and recording 0605

L

Lawyers, defense, civilians, clearance before disclosure to 0916
Legislative recommendations, policy on disclosures concerning 0915
Lettering, size and color used for marking classification 0423, 0427
Letters of transmittal (see also Mail):
classification 0407
marking 0424
Light-gage sheet-metal containers, value ..... Ch. 6, sec. 1, table A
Limited area, definition and requirements ..... App. J
Listening devices, inspection of premises for 0616, 0931
Lists (see Records)
Local alarm system, information on ..... App. I, 6d
Locks:
combination, conventional, definition ..... Ch. 6, sec. 1, table A
combination, manipulation-proof, definition ..... Ch. 6, sec. 1, table A
protective capabilities of various types ..... Ch. 6, sec. 1, table A
Long title, definition 0227
Loss:
disciplinary action in cases of 0805
reporting 0801

M

Mail (see also Armed Forces Courier Service):
addresses, sources of 0711
addressing 0710
bulky packages, inspection prior to transmittal 0710
encrypted and clear-text versions of messages not transmitted under same cover 1304
marking classification on pages of letters 0421
personal. censorship 0909, 0912
registered, for transmission of Secret and Confidential within Continental Limits U. S. 0702
system, Canadian, use of excepted for certain classified material 0703
system, foreign governments, use prohibited except as specified 0703
Top Secret transmission by prohibited 0701
Manipulation-proof combination locks, definition ..... Ch. 6, sec. 1, table A
Manuscripts, marking 0421

Article No.

Maps:
aerial, classification and release ... 1106
marking ... 0421
Marine Corps control of photographs ... 1108
Marking:
classification change ... 0426
classified material received from foreign governments ... 0431
commercial or industrial proprietary material ... 0428
containers for transmission ... 0710
definition ... 0228
endorsements ... 0424
equipment ... 0422
for automatic downgrading ... 0425
general ... 0421
limitations on reproduction of Top Secret ... 0420
material disseminated outside Executive Branch of the Government ... 0433
material not releasable to foreign nationals ... 0429
material releasable to foreign governments ... 0430
material to be destroyed first in emergency ... 0629
Restricted Data ... 0427
Restricted Data transmitted outside Department of Defense ... 0432
size and color used ... 0423
transmittal letters ... 0424
Meetings (see Conferences)
Memoranda, office marking ... 0421
Merchandise vaults, definition ... Ch. 6, sec. 1, table A
Messages:
category A, handling ... 1304
category AC, handling ... 1304
category B, accounting for ... 0611
category B, edited plain-text copies, destruction ... 1304
category B, handling ... 1304
category B, stowage requirements ... 0603
destruction ... 0623, 1304
encrypted and clear-text versions not transmitted under same cover ... 1304
marking ... 0421
responsibility for ... 1301
Microfilm, marking ... 0421
Motion-picture film (see Film)
Munitions of war, definition ... 0229

N

National agency check:
requests for ... 1513
requirements ... 1502
NATO material, Armed Forces Courier Service for certain ... 0709

Article No.

Need-to-know, definition of term 0230
Negatives:
commercial, release of 1103
regraded, marking 0426
rolls of, marking 0421
Newspapers (see also Public news media):
ship and station, publication 1010
Numbering:
additional plain-text copies of category B messages 1304
copies of Top Secret documents 0420, 0607, 0906
Numerical evaluation system for stowage:
definitions of terms used ..... Ch. 6, sec. 1, table A
information on 0602
table of numerical equivalents ..... 0602; Ch. 6, sec. 1, table A

O

Offices, ground-floor, precautions for protection 0616
Operations unusually sensitive, security measures 0912
Original classification authority:
authority for 0401
definition 0231
Originator, definition 0232
Outer containers, addressing and marking 0710
Overclassification:
downgrading and declassifying in cases of 0413, 0414
prevention 0402, 0403, 0406

P

Packages, bulky, inspection 0710
Pages, printed or longhand, marking 0421
Pamphlets, marking 0421
Pay upon restoration to duty after suspension or termination for security reasons ..... App. G
Penalties:
gathering, transmitting, or losing defense information ..... App. D, secs. 793–794
harboring or concealing persons ..... App. D, sec. 792
unauthorized photographing and sketching defense installations ..... App. D, secs. 795–796
unauthorized photographing and sketching vital installations and equipment ..... App. E
unauthorized publication and sale of photographs of defense installations ..... App. D, sec. 797
violations of Atomic Energy Act of 1954 ..... App. B, Ch. 18
violations of security regulations and orders ..... App. H, sec. 21
Personal censorship a fundamental duty 0909
Personal responsibility for prevention of access by unauthorized persons 0613
Personnel clearance (see also Clearance):
criteria 1505
cryptographic material 1303, 1511

464175ms—58——18

Article No.

Personnel — Continued
definition 0233, 1503
granting and recording 1504
immigrant aliens, investigative requirements 1507
previous, reciprocal acceptance policy 1514
termination, reporting 1515
types of 1503
U. S. citizens, investigative requirements 1506

Personnel investigations:
criteria for ..... App. C, sec. 8
previous, reciprocal acceptance policy 1514
reports on, confidential nature ..... App. C, sec. 9
requests for 1513
requirements for Government employment ..... App. C, sec. 3
responsibility for 1501
security investigations index maintained by CSC ..... App. C, sec. 9
types of 1502
Paraphrasing category B messages 1304

Photographs (see also Film; Negatives; Pictures):
adviser to photographers 1104
aerial, classification and release 1106
aerial, unauthorized, use of aircraft prohibited for making ..... App. D, sec. 796
by commercial photographers, submission for review 1103
by naval personnel and contractors, authorization required 1102
control of, responsibility for 1101
defense installations, permission required for ..... App. D, sec. 795
defense installations, unauthorized publication and sale prohibited ..... App. D, sec. 797
Marine Corps control of 1108
vital military and naval installations and equipment, authorization required ..... App. E
Photomaps, marking 0421
Physical security protection for conference quarters 0616, 0931
Pictures, miscellaneous, control of 1109

Plates:
classification or destruction 0614
regraded, marking 0426
Post-card receipt forms, use 0712
Pouches (see Diplomatic pouch)
Premises, inspection for listening devices 0616
Press (see Public news media)

Printing:
facilities approved for 1204
industrial, security 1203
responsibility for 1201
security application 1202
Priority for emergency destruction 0628
Prisoners of war, instructions for 0913

Article No.

Procurement of new forms ..... App. A
Proofs, regraded, marking 0426
Proprietary information:
marking 0428
release policy 0924
Public news media:
classified information not released to 1002
cryptographic data not released to 1007
effect of releases to 1005
information permitted for release to 1003
joint interest information, policy on release to 1004
photographs by representatives of, review 1103
responsibility for release to 1001
Restricted Data prohibited to 1006
Publications (see also Registered publications):
planning, preparation, printing, reproduction, and distribution, responsibility for 1201
Pulping method for destruction of classified material 0623

Q

"Q" clearances 0903, 1512

R

Radio (see Public news media)
Receipts:
category B messages 0611
category B messages, additional plain-text copies 1304
Confidential material 0712
publications distributed through RPS 0712
registered mail transmitted between U. S. and certain Canadian Government installations 0703
Secret material 0608, 0712
Top Secret material 0607, 0712
transfer of material to reliefs 0620
Reception rooms for visitors 0614
Reclassification (see also Downgrading):
definition 0234
marking 0426
notification of 0415
recipient to request 0416
training film 0419
upgrading, definition 0245
Recordings, sound, marking 0421
Records:
Certificates of Clearance 1504
classified material carried by individuals traveling 0705

Article No.

Records — Continued
combinations of safes and vaults, maintenance ... 0605
court-martial proceedings ... 0916
disclosure of Top Secret, forms for ... 0905
individuals afforded access to Top Secret ... 0905
location of classified material, etc., for emergency destruction ... 0627, 0629
use in civil courts ... 0917
visitors, maintenance ... 1405
Records management centers, transfer to ... 0618
References, classification ... 0406, 0411
Registered mail (see Mail)
Registered material:
cryptographic, stowage ... 0603
transmission ... 0707
Registered publications:
accounting for ... 0610
Armed Forces Courier Service for ... 0709
destruction ... 0623, 0626
emergency destruction ... 0628
loss, compromise, or unauthorized disclosure, reporting ... 0801
marking ... 0421
preparation, printing, and reproduction ... 1204
Regrading (see Reclassification)
Release (see Separation)
Relief officers, transfer of classified material to ... 0620
Relocking devices, value ... Ch. 6, sec. 1, table A
Reports:
foreign governments', reclassification ... 0414
loss, compromise, or unauthorized disclosure ... 0801
personnel investigation, confidential nature ... App. C, sec. 9
subversive activities ... 0802
termination of clearance ... 1515
visitors expressing undue interest in classified information ... 1406
Reproductions (see also Printing):
marking assigned classification ... 0421
originator may limit ... 0906
Top Secret, marking limitations ... 0420
Requisitioning new forms, procedure for ... App. A
Reserve personnel:
inactive, unauthorized disclosure to prohibited ... 0907
on active training duty, access permitted if cleared ... 0908
Restricted Data:
definition ... 0305; App. B, Ch. 2
dissemination ... 0903; App. B, Ch. 12
dissemination to inactive reservists prohibited ... 0908
loss, compromise, or unauthorized disclosure, reporting ... 0801

Article No.

Restricted Data — Continued
marking classification 0427
marking containers for 0710
personnel clearances for 1512
preparation, printing, and reproduction 1204
release to public prohibited 1006
stowage 0604
Top Secret, originated by Atomic Energy Commission, accounting for 0612
transmission 0706
transmitted outside Department of Defense, marking 0432
unlawful dissemination, penalties for ..... App. B, Ch. 18
Retired personnel, unauthorized disclosure to prohibited 0907
Reverse sides of pages, marking 0421

Rooms:
heavily constructed, definition ..... Ch. 6, sec. 1, table A
lightly constructed, definition ..... Ch. 6, sec. 1, table A
reception, for visitors 0614
vacated during working hours, stowage of classified material 0614

S

Sabotage, reporting 0802

Safes (see also Combination locks; Combinations; Stowage containers):
relocking devices, value ..... Ch. 6, sec. 1, table A
steel, heavy, definition ..... Ch. 6, sec. 1, table A
steel, light-weight, definition ..... Ch. 6, sec. 1, table A

Sale:
classified documents, prohibition 1205
photographs of defense installations, prohibition ..... App. D, sec. 797
Screens for ground-floor office windows 0616

Secret:
accounting for 0608
authority to classify 0401
bulky material, transmission 0708
certificates of destruction for 0625
classification denotes vital military and naval installations and equipment ..... App. E
clearance, U. S. citizens, investigative requirements 1506
communication material, emergency destruction priority 0628
definition and use 0303
destruction 0623
dissemination to Reserve personnel for training, policy on 0908
lettering used for marking 0423
preparation, printing, and reproduction 1204
stowage requirements evaluation graph ..... Ch. 6, sec. 1, table B
transmission within Continental Limits U. S. 0702

Article No.

Security (see also Communication security):
application of ... 0103
areas, information ... App. J
checks at close of each working day ... 0615
control measures, limitations ... 0105
definition ... 0237
instructions, basis for ... 0104
instructions, issuance to meet local situations ... 0107
interpretation, general ... 0107
measures required for various types of security areas ... App. J
objective of ... 0102
penalties for violations of regulations ... App. H, sec. 21
principle, circulation control ... 0106
requirements for Government employment ... App. C
responsibility for ... 0101; App. C, sec. 2
unusually sensitive operations ... 0912
Security classification (see Classification)
Security clearance (see Clearance; Personnel clearance)
Sensitive operations requiring extraordinary security measures ... 0912
Sensitive positions, designation and filling ... App. C, sec. 3

Separation:
action to be taken upon ... 0619, 0909
changing safe and vault combinations after ... 0605
in the interests of national defense ... App. C, sec. 6; App. G
Sheet-metal containers, light-gage, value ... Ch. 6, sec. 1, table A
Shipment of bulky material ... 0708

Ships:
collisions, surveys prohibited in certain cases ... 0919
new construction, visits to ... 1411
security during visits ... 1409, 1410
visits by foreign personnel ... 1410

Short title:
classification ... 0411
definition ... 0238
Shrubbery outside ground-floor offices, trimming ... 0616
Single classification for each document ... 0407
Size of lettering used for classification marking ... 0423, 0427

Sketches:
control of ... 1109
defense installations, permission required for ... App. D, sec. 795
vital military and naval installations and equipment, authorization required ... App. E
Sound recordings, marking ... 0421
Spaces (see Areas)
Special equipment, marking ... 0422
Special handling notices, use ... 0429
Speeches, classified information not to be included in ... 1009

Article No.

Sponsorship:
definition 0239
Navy, of conferences and meetings 0929, 0932
Standard forms required, requisitioning 0108
Steel filing cabinets:
combination-lock, value ..... Ch. 6, sec. 1, table A
key-lock, value ..... Ch. 6, sec. 1, table A
Steel safes:
heavy, definition ..... Ch. 6, sec. 1, table A
light-weight, definition ..... Ch. 6, sec. 1, table A
Stencils, classification or destruction 0614
Stenographic notes, classification or destruction 0420, 0614, 0615
Stocks, bulk, or regraded documents, marking 0426
Stowage:
classification review before transfer for 0417
definition 0240
during fire alarms or other emergencies 0617
if room is vacated during working hours 0614
inspection at close of each working day 0615
numerical evaluation system for 0602
publications on board ships, accessibility for destruction 0629
requirements 0601
requirements evaluation graph ..... Ch. 6, sec. 1, table B
Stowage containers (see also names of specific types; Safes, Vaults, etc.)
changing and recording keys and combinations 0605
closed or open, value of control of personnel access to ..... Ch. 6, sec. 1, table A
found open, action to be taken in case of 0606
person responsible for, identity readily available 0615
value of various types ..... Ch. 6, sec. 1, table A
Subversive activity, reporting 0802
Surrounding areas separately protected, value ..... Ch. 6, sec. 1, table A
Surveys of ships' collisions, prohibition in certain cases 0919
Suspension of Government employees in the interests of national defense ..... App. C, sec. 6; App. G
Symposia (see Conferences)

T

Tables:
evaluation graph, minimum levels of required stowage protection ..... 0602; Ch. 6, sec. 1, table B
numerical equivalents for stowage protection ..... Ch. 6, sec. 1, table A
requirements for processing visitors who will have access ..... Ch. 14, sec. 3, table C
Tampering:
courier mail, reporting evidence of 0803
from outside ground-floor offices, prevention 0616
Tapes, composition, marking 0421

Article No.

Technical equipment, downgrading 0418
Technical information, definition 0241
Telephone discussion of classified information prohibited 0614, 0909, 0910
Television (see Public news media)
Testimony before congressional committees 0914
Title or subject, classification of 0409
Title page, marking 0421

Top Secret:
- accounting for 0607
- Armed Forces Courier Service for 0709
- authority to classify 0401
- bulky material, protection of shipments 0708
- certificates of destruction for 0625
- classification denotes vital military and naval installations and equipment ..... App. E
- clearance, U. S. citizens, investigative requirements 1506
- communication material, emergency destruction priority 0628
- controls for 0905
- copies and extracts, control of 0906
- definition and use 0302
- destruction 0623
- dissemination to Reserve personnel for training, policy on 0908
- lettering used for marking 0423
- preparation, printing, and reproduction 1204
- preparation and marking 0420
- releasable to foreign governments, marking 0430
- Restricted Data originated by Atomic Energy Commission, accounting for 0612
- stowage requirements evaluation graph ..... Ch. 6, sec. 1, table B
- transmission within Continental Limits U. S. 0701

Top Secret control officer:
- designation 0503
- duties 0504

Tracings, marking 0421
Traffic, international, in arms, administration by State Department 0922
Training, foreign nationals 0921

Training film:
- contracts for 1105
- defense classification, procedure for changing 0419

Transmission, definition 0243

Transmittal letters:
- classification 0407
- marking 0424

Transportation, commercial, of bulky material 0708
Travel, protection of classified material during 0705
Trials, prevention of unauthorized disclosures at 0916

Article No.

U

Unauthorized disclosure:
disciplinary action in case of 0805
reporting 0801
Unauthorized persons:
definition ..... 0213; App. F
oral discussions with prohibited 0909
Unbound documents:
definition 0244
regraded, marking 0426
Upgrading, definition 0245

V

Vaults (see also Stowage containers):
bank, definition ..... Ch. 6, sec. 1, table A
light, definition ..... Ch. 6, sec. 1, table A
merchandise, definition ..... Ch. 6, sec. 1, table A
relocking devices, value ..... Ch. 6, sec. 1, table A
Violations:
containers found open, action taken 0606
disciplinary action in cases of 0805
not resulting in loss, compromise, or unauthorized disclosure, handling 0804
reporting 0801–0803
security regulations, penalties for ..... App. H, sec. 21
Visitors:
access, information required for 1415
access, interpretation of term 1414
categories 1403
classified visits ..... Ch. 14, sec. 3
clearances when access is authorized 1414
definition 1402
documents not released to 1417
escorts for 1405, 1407, 1408
foreign nationals, Navy sponsorship 1413, 1419
general visiting 1409
identification 1416
photographic equipment prohibited unless authorized 1101
reception rooms 0614
records of 1405
reports on certain 1406
responsibility for security control of 1401, 1404
ship security during visits 1409, 1410
ships, visit to by foreign personnel 1410
ships under construction 1411

Article No.

Visitors — Continued
to foreign countries, Navy sponsorship ... 1412, 1418
unclassified visits ... Ch. 14, sec. 2
Vital military and naval installations and equipment, definition ... App. E, 1–3

W

War prisoners, instructions for ... 0913
Waste material, destruction ... 0623
Wastebaskets, stowage or destruction of contents ... 0615
Weight of stowage containers, security value ... Ch. 6, sec. 1, table A
Wire circuits approved for transmission of Secret and Confidential ... 0911
Witnesses for destruction of classified material ... 0623, 1304
Wooden containers, value ... Ch. 6, sec. 1, table A
Working spaces, care of ... 0616
Worksheets, classification or destruction ... 0401, 0420, 0614, 0615
Wrappings for transmission, sealing and marking ... 0710

U. S. GOVERNMENT PRINTING OFFICE : 1958—464175